PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRIA EN REDES DE COMUNICACIONES

TRABAJO PREVIO LA OBTENCION DEL TÍTULO DE:

MAGÍSTER EN REDES DE COMUNICACIÓN

TEMA:

"DESARROLLO DE PROCEDIMIENTOS PARA UN MODELO DE GESTION DE FALLAS DE LA RED PARA LA PLATAFORMA ISP DE LA CNT EP"

AUTOR:

Ing. Jessica Alexandra Cruz Villa

DIRECTOR:

Carlos Egas Acosta Master

QUITO, NOVIEMBRE 2015

AUTORIA

Yo, Ing. Jessica Alexandra Cruz Villa, portadora de la cédula de ciudadanía No. 1717000630 declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

Ing. Jessica Alexandra Cruz Villa

AGRADECIMIENTO

Agradezco a Dios quien me ha acompañado y ha puesto en mí el Espíritu Santo permitiéndome culminar esta etapa en mi vida. A la Pontificia Católica del Ecuador en especial a los profesores Carlos Egas Acosta, Gustavo Chafla y Juan Francisco Chafla por los conocimientos impartidos los cuales fueron aplicados en la realización del presente trabajo. Germán Célleri pues me brindó las facilidades para ejecutar este trabajo y a la Corporación Nacional de Telecomunicaciones. También a mis Padres, Esposo y Hermanas, quienes me han manifestado un continuo apoyo, han sido un soporte y pilar fundamental.

DEDICATORIA

Dedico este trabajo a Dios, mis Padres, Esposo, Hermanas, y también a Germán Célleri quienes con su paciencia y guía colaboraron para la culminación de este proyecto.

CONTENIDO

RESUMEN

Desarrollo de Procedimientos para un modelo de Gestión de Fallas de la Red para la plataforma ISP de la CNT EP cuyo alcance abarca el equipamiento de comunicaciones (equipos routers) que conforman la plataforma de ISP de CNT EP. Se trabajó con la herramienta de monitoreo de red CACTI desde la cual se obtiene los principales indicadores de falla por equipo, y se monitorea los mismos. El modelo de Gestión de fallas se elaboró de acuerdo a la descripción realizada de cada función de gestión de fallas, los niveles de criticidad, la clasificación de los niveles de criticidad por Indicador, los valores para reportar un indicador de falla, y se ensayó lógicamente los procesos definidos para la Gestión de Fallas.

Con los resultados obtenidos se verifica que al existir un modelo de Gestión de Fallas éste permite enfocar las funciones de cada área dentro de la estructura organizacional de la empresa al igual que realizar actividades sin duplicar las mismas entre las áreas.

Se concluye que este modelo permitirá a la empresa contar con una Gestión de Falla para el ISP ofreciendo la posibilidad de realizar acciones para detección, diagnóstico y reparación de fallos mejorando los tiempos de atención de incidencias, la disponibilidad de la red.

Se recomienda que éste modelo sea considerado por la empresa y de ser aprobado sea implementado como un sistema de cumplimiento obligatorio para la Operación y Mantenimiento de plataformas dentro de la organización.

ABSTRACT

Procedures for developing a model of Fault Management Network for the ISP platform CNT EP whose scope covers the communications equipment (routers devices) that make up the platform of CNT EP ISP. We worked with the network monitoring tool CACTI from which the main fault indicators per team is obtained, and the same is monitored. The fault management model was developed in accordance with the description of each function fault management, levels of criticality classification levels of criticality indicator values to report a fault indicator, and tested logically defined processes for Fault Management.

With the results verified that the absence of a fault management model allows it to focus the functions of each area within the organizational structure of the company as well as activities without duplicating the same between areas.

We conclude that this model will allow the company to have a management failure for the ISP providing the ability to perform actions for detection, diagnosis and repair of failures to improve service times of incidents, the availability of the network.

It is recommended that this model be considered by the enterprise and if It is approved, It will be implemented as a mandatory system for the Operation and Maintenance of platforms within the organization.

1. CAPITULO I.-

1.1 ANTECEDENTES

La CNT EP tiene un área que es un ISP ó Proveedor de Servicio de Internet la cual provee del servicio de Internet a nivel Nacional. Esta área mantiene una plataforma que está constituida por equipos de diferentes proveedores como Ruteadores, Switch (CISCO), DNS64.

La estructura organizacional de la CNT EP está compuesta por:

Gerencia Coordinadora de Operación y Mantenimiento: es la que coordina con las gerencias bajo su nivel para gestionar temas administrativos y son las siguientes: [1]1.

- Gerencia de O&M: dentro de esta gerencia se encuentra la Jefatura de O&M ISP en la cual se encuentra la plataforma del ISP de la CNT EP y es la responsable de Operar, Mantener y Garantizar la disponibilidad de la prestación del servicio de Internet al igual que la plataforma.

- Centro de Operación de Red: se encarga del monitoreo de red y análisis de disponibilidad de servicios, tráfico, desempeño de los equipos y plataformas

[1] Referencia bibliográfica [1] (CNT, 2014)

que conforman la Red de CNT EP, en específico la red del ISP. Esta Gerencia está compuesta por las Jefaturas:

  - Desempeño de red, la cual se encarga de coordinar con el área de Ingeniería para implementar mejoras, ampliaciones o compras para solventar los inconvenientes que presentan vulnerabilidades en los equipos o plataformas de comunicaciones de ISP los cuales pueden ocasionar fallas de los mismos.
  - Centro de Operaciones de Red (NOC), la cual se encarga de monitorear la red de equipos o plataformas de comunicaciones de ISP.

- Gerencia de Transmisiones: es la responsable de brindar la interconexión entre las diferentes centrales mediante anillos metropolitanos, a nivel nacional Fibra Óptica, y MPLS.

Gerencia de Ingeniería e Implementación: es la que coordina con las gerencias bajo su nivel para gestionar temas administrativos y son las siguientes:

- Gerencia de Ingeniería: se encarga de diseñar, definir procesos de mejoramiento, optimización o ampliación de Red, y para los casos en los cuales sus diseños requieran adquirir mediante procesos de compra equipamiento e implementar las mejoras o ampliaciones de red del ISP.

El ISP de la CNT EP en la estructura operacional está bajo la Gerencia Coordinadora de Operación y Mantenimiento dentro Gerencia de O&M Centrales y Plataformas.

Los análisis de fallas de los equipos se realizan de manera reactiva, es decir solo en caso de que un evento ocurre y afecte la normal operación, además existen también documentos SLA (Niveles de acuerdo de servicio) que se encuentran relacionados con el nivel del servicio y la metodología empleada para determinar los valores permisibles de los indicadores de dicho nivel. El ISP de la CNT EP actualmente no cuenta con un proceso de análisis de fallas que ayude a mejorar la obtención de los indicadores de disponibilidad, y los procesos de análisis de fallas. Por lo cual es necesario como parte fundamental de los análisis de disponibilidad y fallas de la red establecer los procedimientos de un modelo de gestión de fallas.

1.2 JUSTIFICACIÓN

En base al antecedente existe la necesidad de desarrollar los procedimientos de gestión de fallas para la plataforma ISP de la CNT EP y su alcance es el desarrollo de procedimientos de un modelo de gestión de Fallas para el equipamiento de comunicaciones (routers) que conforman la plataforma de ISP.

El desarrollo de los procedimientos del modelo de gestión de fallas del equipamiento de comunicaciones (routers) que conforman la plataforma de ISP,

permitirá contar con procesos adecuados para mejorar la disponibilidad, optimización de tiempos de atención a una falla, mejorar niveles del servicio que brinda el ISP y deberá contar con una adecuada herramienta como un gestor centralizado de fallas para incrementar su eficiencia.

1.3 OBJETIVOS

El objetivo general de este trabajo es desarrollar los procedimientos de un modelo de gestión para el proceso de atención de fallas del equipamiento de comunicaciones (routers) que conforman la plataforma de ISP.

1.3.1 OBJETIVOS ESPECIFICOS

- Desarrollar las actividades del proceso de atención de fallas ocurridas sobre el equipamiento de comunicaciones (routers) que conforman la plataforma de ISP de la CNT EP.

- Desarrollo del procedimiento para las alarmas definidas sobre el equipamiento de comunicaciones (routers) que conforman la plataforma de ISP de la CNT EP.

- Aplicar en la práctica el modelo de gestión con sus procedimientos a un grupo de fallas ocurridas sobre el equipamiento de comunicaciones

(routers) que conforman la plataforma de ISP de la CNT EP.

1.3.2 BENEFICIOS ESPERADOS

Con la implementación de este modelo de Gestión de Fallas se espera obtener los siguientes beneficios:

- ✓ Mejorar los tiempos de atención de incidencias.
- ✓ Mejorar la disponibilidad de la red.
- ✓ Optimizar el recurso humano para el soporte de incidencias
- ✓ Facilitar al operador el manejo de los incidentes
- ✓ Ahorro de costos por causas de SLA incumplidos
- ✓ Crear cultura de manejar procedimientos de gestión para actividades de los equipos de comunicaciones (ruteadores) de la red de ISP.

1.4 ALCANCE

Esta tesis se encuentra orientada en diseñar los procedimientos de un modelo para la gestión de fallas del equipamiento de comunicaciones (routers) que conforman la plataforma de ISP de la CNT EP e incluye una implementación práctica del modelo utilizando una herramienta de gestión disponible para que pueda ser usado en la Jefatura de O&M de Core y Plataformas de Intenet, TV y Datos.

Un modelo de gestión en el sistema ISO tiene tres componentes básicos: Modelo Organizacional, Modelo Técnico y Modelo Funcional. Este proyecto de tesis se limita al componente denominado Modelo Funcional.

El componente Funcional cuenta a su vez con los siguientes Procesos y Procedimientos: [1][2]

1. Gestión de configuración
2. Gestión de fallas
3. Gestión de rendimiento de red
4. Gestión de seguridades
5. Gestión de carga y confiabilidad
6. Gestión de Planificación

De acuerdo a los antecedentes y justificativo de este proyecto el modelo en el cual se trabajará es el de Gestión de Fallas.

Gestión de Fallas: Es un conjunto de actividades para mantener dinámicamente el nivel de servicio de la red.

[2]Referencia bibliográfica [1](EGAS, 2007)

Gestión de Fallas consiste en:

- Detección de la ocurrencia de fallas
- El aislamiento de la causa de la falla
- La corrección de la falla

Gestión de Fallas se encarga de:

- Supervisión de alarmas
    - Indicación de fallas
    - Naturaleza y gravedad
- Localización de fallas
    - Rutinas para la localización
- Pruebas
- Corrección de Fallas
    - Emitir reportes de fallas ocurridas

Las principales Funciones de la Gestión de Fallas son:

- Supervisión del estado de la red
- Rastreo dinámico de los problemas

- Detección de problemas
- Respaldo y reconfiguración
- Diagnóstico y reparación
- Pruebas punta a punta

De este modelo de gestión en el presente trabajo se limita a:

Gestión de Fallas que consiste en:

- Detección de la ocurrencia de fallas

Las principales Funciones de la Gestión de Fallas son:

- Supervisión del estado de la red
- Detección de problemas
- Respaldo y reconfiguración
- Diagnóstico y reparación

Los procesos de gestión de fallas se realizarán sobre equipamiento de comunicaciones (routers) que conforman la plataforma de ISP de la CNT EP en Quito y estos podrán ser replicados en el sitio de Guayaquil, tomando en cuenta que es una copia espejo de arquitectura implementada con fines de redundancia geográfica.

1.5 NECESIDAD DE UNA GESTIÓN DE FALLAS DEL ISP

En la actualidad en la empresa el área NOC de acuerdo a la nueva estructura realiza funciones de monitoreo de la red, se ha detectado que al no tener un procedimiento de gestión de Fallas para el equipamiento o plataforma administrado por cada área responsable, realiza comunicaciones de alertas a las áreas que considera involucradas, esto ocasiona a que los tiempos de respuesta para la atención de esas fallas sean muy extensos, esto es, porque cada área revisa su plataforma descarta eventos en la misma y devuelve el reporte a NOC y hasta que el área que tiene la falla identifique la misma han pasado más de 2 a 3 horas.

Se busca optimizar los tiempos de atención de fallas ante incidentes reportados por el NOC, es decir, si NOC ya dispone de una guía para identificar las fallas en una plataforma o equipamiento puede enviar directamente el evento de atención al área correcta ahorrando por lo menos dos horas.

Para lograr esa optimización de tiempos se propone empezar por esta área ISP a través de una Gestión de Fallas en los equipos de comunicaciones, ya que el querer implementar este proceso en la Gerencia de Operación y Mantenimiento se vuelve complejo. La complejidad de implementar este sistema de Gestión de Fallas en Operación y Mantenimiento se da porque, abarca varias gerencias técnicas con sus

respectivas jefaturas y actualmente ya se dispone de una estructura organizacional implementada con sus respectivas actividades en las cuales no consta la aplicación de este proceso de gestión.

Como lo había explicado anteriormente ya existe un área que se encarga del monitoreo de red la cual se entendería debería estar enfocada en procesos de gestión de fallas pero en la realidad trabaja con actividades que de acuerdo al criterio del responsable del área debería ser, no existen procedimientos establecidos que regulen a todas las áreas técnicas y NOC, a que me refiero con esto, a que el proceso de Gestión de Fallas se aplica de acuerdo a cada criterio como le funcione y no a un proceso establecido.

Para que el proceso de Gestión de Fallas sea fundado y aplicado en todas las áreas implica la intervención de la Gerencia de Desarrollo Organizacional la cual dispone el cumplimiento de éstos, esta es otra complejidad identificada para implementar el sistema de Gestión de Fallas en la organización en la Gerencia Técnica.

Con estos antecedentes y con el fin de evitar la afectación de la prestación de servicio de Internet ocurrida por eventos en equipos de comunicaciones del ISP como por ejemplo fallas de apagado de los equipos, sobrecarga del CPU, sobrecarga de la memoria, daños físicos en la interfaz del equipo etc. los cuales pueden ser

prevenidos mediante la detección de fallas de manera proactiva o mitigación, y por razones de costos, productividad es más conveniente mantener la capacidad de funcionamiento de los mismos actuando de forma preventiva, se ve necesario poseer procedimientos de gestión de fallas en la red del ISP.

Para esto, el mantenimiento puede contribuir en gran medida a la conservación y reutilización de los recursos físicos, la experiencia enseña que más o menos el 50% de las fallas producidas por desgaste en los equipos se pueden evitar con medidas adecuadas de mantenimiento. Por lo que es necesario que la empresa tome conciencia de la importancia que tienen los trabajos de mantenimiento basados en indicadores de falla tratando que se ponga en práctica las medidas efectivas que significan realizarlo.

Con este trabajo se quiere aportar al desarrollo de una Gestión de Fallas de la red del ISP, estableciendo indicadores de fallas, procedimientos relacionados al mantenimiento, niveles de criticidad y valores para reportar una falla.

El alcance de este trabajo contempla el tratamiento teórico del modelo de gestión de fallas, establecimiento de los indicadores de falla, elaboración de los procedimientos a aplicar en base a los indicadores de falla establecidos, los cuales están basados de acuerdo a la estructura orgánica funcional y sus respectivas

funciones, implementación del monitoreo de los indicadores de falla en los equipos de comunicaciones del ISP usando una herramienta de gestión.

Este trabajo una vez culminado pueda ser aplicado ya que los indicadores, procedimientos, y todo lo que conlleva el modelo de Gestión de Falla se desarrollarán sobre la estructura organizacional vigente y equipamiento existente en la actualidad. De igual manera puede contribuir para implementar este sistema de Gestión de Fallas en las demás áreas si así lo requieren.

También será expuesto en DEO (Desarrollo Organizacional) para que sea considerado y de ser favorable se aplique como un sistema de cumplimiento obligatorio para la Gerencia Técnica dentro de la organización.

1.6 DESCRIPCIÓN DE LA RED DE COMUNICACIONES DEL ISP DE LA CNT EP

1.6.1 Arquitectura de red

El esquema indicado en la Gráfia1.6.1 fue implementado en el área de ISP luego de un trabajo en conjunto con las áreas técnicas de operación & mantenimiento e ingeniería, quienes en busca de mejorar la disponibilidad de los servicios, como parte de la nueva arquitectura ya que en su mayoría ISP administra equipos de marca CISCO revisaron los modelos propuestos por éste. (CISCO, 2010)

CISCO maneja un modelo jerárquico que consta de 3 capas en las cuales se define funciones en cada una de ellas permitiendo así poder aplicar de una manera ordenada configuraciones en la red, cada capa tiene funciones específicas asignadas las cuales no necesariamente están separadas de manera física si no de manera lógica, esto permite mantener diferentes equipos en una sola capa o un equipo haciendo las funciones de más de una de las capas.

Para CISCO las funciones de cada capa se resumen de la siguiente manera: [1][3]

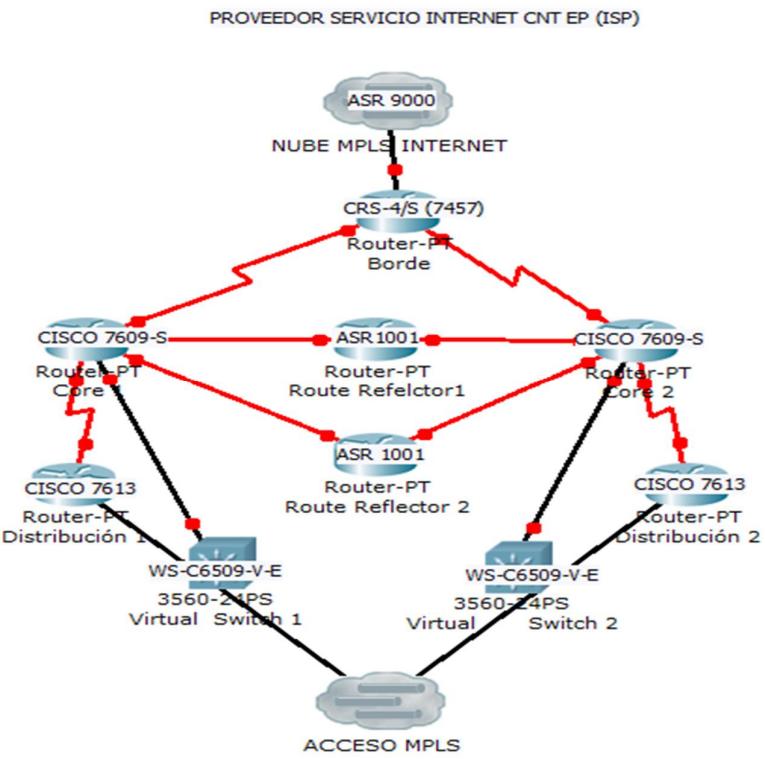
- Capa de Acceso: se la conoce también como capa de conmutación (switching), permite la conexión a los equipos finales controlando la comunicación entre ellos en la red. En esta capa de acceso puede operar equipos routers, switches, puntos de acceso inalámbrico.

- Capa de Distribución: Recibe y añade la información que envía los equipos de la capa de acceso antes de trasmitirlos a la capa núcleo, controla el flujo de tráfico de la red con el uso de políticas, facilita ruteo, filtrado, define dominios de broadcast para realizar el enrutamiento entre las VLAN definidas en la capa de acceso.

[3]Referencia bibliográfica [1] (CISCO, 2010)

- Capa Núcleo: se la considera como backbone donde de añade el tráfico de todos los equipos de la capa distribución, maneja gran cantidad de tráfico de manera confiable y veloz. La función principal en esta capa es el conmutar tráfico.

En la Gráfica1.6.1 se muestra el Diagrama de la red de comunicaciones del ISP el cual por temas de seguridad de la información se presenta con nombres genéricos, no incluye direccionamiento IP, se muestra el esquema de capas en este caso 3 y se detalla a continuación:



Gráfica1.6.1 Diagrama de la red de comunicaciones del ISP.

Como se puede observar en la Gráfica1.6.1 el ISP de la CNT EP se encuentra operando en un esquema de 3 capas al igual que cisco pero de manera personalizada:

- BORDE: Esta capa se encarga de enviar y recibir el tráfico de Internet hacia el backbone de Internet. Permite interconectar indirectamente al ISP hacia la red Internet de los proveedores denominados Tier1[4] los cuales son proveedores de conectividad hacia el backbone mundial de Internet. En esta capa se configura E-BGP para comunicarse con el sistema autónomo del backbone de Internet.

- CORE: Esta capa concentra todos los servicios que brinda ISP tales como hosting, correo electrónico, internet, caché, DNS. También concentra todo el tráfico de Internet que no se queda en la capa de acceso para el envío hacia la capa de borde. En esta capa de configura I-BGP para comunicarse entre equipos con el sistema autónomo del ISP.

- DISTRIBUCIÓN: esta capa es semejante a la capa de acceso en CISCO, concentra el acceso de las redes de los clientes corporativos, masivos. En esta capa se recibe el tráfico de las denominadas VRF (enrutamiento virtual

[4] Tier 1 es un ISP que tiene acceso a toda la Región de Internet (internacional) exclusivamente a través de sus acuerdos de peering gratuitos y recíprocas.

y reenvío), lo cual permite múltiples instancias de una tabla de enrutamiento para coexistir en el mismo router, debido a que las instancias de enrutamiento son independientes, se pueden utilizar sin entrar en conflicto entre sí, direcciones IP comunes. En esta capa se configura I-BGP para comunicarse entre equipos internos del sistema autónomo del ISP.

La comunicación entre los equipos del ISP es a través de la configuración del protocolo ISIS, el cual permite ver las loopbacks y wan`s entre los mismos equipos, estableciendo conexiones entre ellos y de esa manera configurar BGP entre los equipos hacia los RouterReflectors y viceversa. Para el balanceo de tráfico se configuran métricas.

El ISP de la CNT EP tiene registrado el sistema autónomo público en LACNIC el cual es exclusivo y permite que pueda ser identificado entre los diferentes sistemas autónomos a nivel mundial. El sistema autónomo sirve también para administración del equipamiento interno del ISP y el tráfico del mismo.

Los denominados sistemas autónomos o AS[5]se interconectan con protocolos de encaminamiento externo como BGPV4[6] anunciando prefijos de red entre AS´s dependiendo de una política de encaminamiento. La política de encaminamiento o

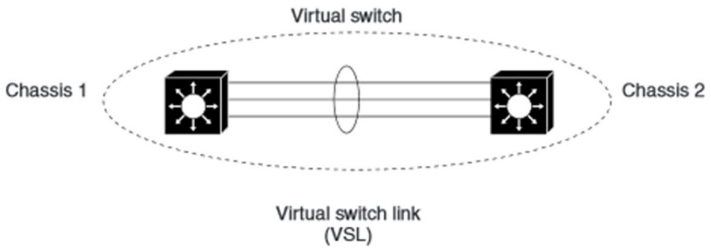
[5] Es una red o conjunto de redes que están administradas bajo un número de identificación global y única.

[6] Protocolo de encaminamiento de información entre AS, usa TCP como transporte de mensajes BGP.

“routing policy” es la decisión del AS de anunciar la red a otro AS y es el privilegio del otro AS el aceptar la información de encaminamiento de forma que pueda transitar el flujo de tráfico.

El ISP de la CNT EP maneja una configuración de escalabilidad en BGP la cual se conoce como Reflectores de rutas ó “Route Reflectors”, en estos equipos se propagan rutas aprendidas de un I-BGP a un I-BGP vecino reduciendo el número de sesiones BGP TCP en el AS. El reflector de rutas propaga una ruta a todos los equipos internos del ISP independientemente si estos están física o lógicamente conectados.

También dentro de la arquitectura del ISP se tiene un esquema VSS o Virtual Switching System el cual es un sistema en cluster que utiliza dos switch de hardware común que actúan como un solo elemento de red compartiendo la información de control y tráfico de datos. Para lograr que los equipos funcionen como uno solo se configura VSL ó Virtual Switch Link, el cual es un vínculo que lleva el control y tráfico de datos entre los dos switches. El VSL se implementa como un Ether Channel también conocido como un port cannel, el cual es un agrupamiento de dos ó más interfaces o enlaces físicos que se combinan para formar un enlace lógico. Las conexiones redundantes entre los dos chasis se realizan usando tarjetas independientes. A continuación se muestra en la Gráfica1.6.2 la conexión entre el VSS y VSL.



Gráfica1.6.2 - VSS y VSL.

En la Gráfica1.6.1 se puede observar también nubes las cuales se detalla a continuación:

- Nube MPLS Internet: esta nube contiene equipos que llevan el tráfico hacia el Backbone de Internet el cual es administrado por el área de TX-MPLS de la CNT EP. A esta nube se interconecta el equipo de BORDER del ISP.

- Acceso MPLS: esta nube hace referencia al conjunto de equipos geográficamente distribuidos a nivel local y nacional, e interconectados mediante una red MPLS para permitir acceso a internet a los clientes masivos y corporativos a los cuales brinda servicio el ISP de la CNT EP.

1.7 EQUIPOS, FUNCIONES Y ESPECIFICACIONES

1.7.1 Equipos

En la Tabla 1.7.1 se muestra el listado de los equipos que conforman el diagrama de la red de comunicaciones de ISP.

NOMBRE	MODELO	MARCA
Borde	CRS-4/S	CISCO
Core 1	7609-S	CISCO
Core 2	7609-S	CISCO
Route Reflector 1	ASR1001	CISCO
Route Reflector 1	ASR1001	CISCO
Distribución 1	7613	CISCO
Distribución 2	7613	CISCO
Virtual Switch 1	WS-C6509-V-E	CISCO
Virtual Switch 2	WS-C6509-V-E	CISCO

Tabla. 1.7.1 Listado de equipos de la red de comunicaciones del ISP.

1.7.2 Funciones

En ISP se implementó una ingeniería por capas, en este caso se aplicó un modelo de 3 capas y cada una cumple una función específica. El equipamiento fue colocado en cada una de ellas en base a un estudio de la capacidad de procesamiento, cantidad de interfaces físicas, protocolos que se puede aplicar, el tráfico que soporta cada uno de ellos.

EQUIPO DE BORDE: La función que realiza este equipo dentro del ISP es llevar y traer el tráfico de internet desde o hacia la nube MPLS Internet a las capas inferiores. En la capa inferior de Core están los servidores de caché que discriminan

tráfico de internet local utilizando algoritmos en sus bases de datos,

El equipo de Borde se conecta con otro router en la nube MPLS Internet, éste equipo cumple la función de interconectar el tráfico de Internet que viene del ISP con los equipos de backbone de Internet MPLS los cuales encaminan el tráfico por los diferentes Tier1.[3]a los que se interconecta CNT EP.

EQUIPO DE CORE: La función de este equipo en el ISP es la de concentrar todo el tráfico que viene desde las capas inferiores o los equipos de borde para que de acuerdo a la configuración de los protocolos de enrutamiento BGP e ISIS distribuya el tráfico al borde o a los equipos de distribución de manera balanceada.

Otra de las funciones del equipo del CORE es conectar los servicios que brinda el ISP tales como: Hosting, Correo electrónico, DNS, Monitoreos.

Una función importante del equipo de CORE es la de conectar los enlaces de transmisión que proveen redundancia entre Quito y Guayaquil a nivel del ISP.

EQUIPOS DE DISTRIBUCIÓN: La función de estos equipos es la de concentrar todo el tráfico de Internet de los clientes masivos y corporativos.

En estos equipos se aplican políticas dedicadas a nivel del cliente, por ejemplo bloqueo de puertos. Es una recomendación hacer el bloqueo a nivel más cercano del cliente, para que no afecte el tráfico en las capas superiores de la red.

ROUTE RELECTOR: la función de estos equipos es la aprender y distribuir rutas o redes a través de BGP e ISIS.

VIRTUAL SWITCH: la función de estos equipos es la de conectar directamente los servicios de valor agregado que brinda el ISP, es parte del CORE.

1.7.3 Especificaciones [2]7

A continuación se detalla las especificaciones básicas generales de los equipos de borde, core, distribución, route reflector, virtual switch, entre ellas: Versión software, Protocolos que soporta el equipo de acuerdo a la versión de software, tarjetas, puertos, ranuras, memoria, rendimiento, las MIB, interfaces de gestión para el equipo, características de energía que se deben tomar en cuenta para encender este equipo y sus condiciones ambientales.

BORDE CRS-4/S CISCO	
Característica	**Descripción**
Versión software	Cisco IOS XR Software, Version 4.1.2[Default]
Protocolos	• Protocolo de descubrimiento de Cisco
	• IPv4 e IPv6

[7] Referencia bibliográfica [2] (CISCO, 2015)

	• Protocolo de mensajes de control de Internet (ICMP)
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• Protocolo de administración de grupos de Internet (IGMP) versiones 1, 2 y 3
	• multiprotocolo BGP (MBGP)
	• Multicast Source Discovery Protocol (MSDP)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• Protocolo de reserva de recursos (RSVP)
	• Servicios diferenciados (DiffServ) ingeniería de tráfico sea conscientes
	• plano de control MPLS Ingeniería de Tráfico (RFC 2702 y 2430)
	• Enrutamiento de Política Lingüística (RPL)
	• Gestión
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• Seguridad
	• Mensaje DigestAlgorithm 5 (MD5)
	• Protocolo (IPsec) de seguridad IP
	• Secure Shell Protocolo (SSHv2)
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
Tarjetas, puertos y ranuras	2 Management Ethernet
	12 WANPHY controller(s)
	12 TenGigE
	1019k bytes of non-volatile configuration memory.
	34338M bytes of hard disk.
	2053440k bytes of disk0: (Sector size 512 bytes).
Memoria	4 GB
Rendimiento	Capacidad de conmutación de 320 Gbps
MIB QUE SOPORTA EL EQUIPO	SNMP frameworksupport
	• SNMPv1
	• SNMPv2c
	• SNMPv3
	• MIB II, including interface extensions (RFC 1213)

	• SNMP-FRAMEWORK-MIB
	• SNMP-TARGET-MIB
	• SNMP-NOTIFICATION-MIB
	• SNMP-USM-MIB
	• SNMP-VACM-MIB
	Systemmanagement
	• CISCO- BULK-FILE-MIB
	• CISCO-CONFIG-COPY-MIB
	• CISCO-CONFIG-MAN-MIB
	• CISCO-FLASH-MIB
	• CISCO-MEMORY-POOL-MIB
	• Cisco FTP Client MIB
	• Cisco Process MIB
	• Cisco Syslog MIB
	• CISCO-SYSTEM-MIB
	• CISCO-CDP-MIB
	• IF-MIB (RFCs 2233 and 2863)
	Chassis
	• ENTITY-MIB (RFC 2737)
	• CISCO-entity-asset-MIB
	• CISCO-entity-sensor-MIB
	• CISCO-FRU-MIB (Cisco-Entity-FRU-Control-MIB)
	Fabric MIB
	• CISCO-Fabric-HFR-MIB
	• CISCO-Fabric-Mcast-MIB
	• CISCO-Fabric-Mcast-Appl-MIB
	Routingprotocols
	● BGP4-MIB Version 1
	● OSPFv1MIB (RFC 1253)
	• CISCO-IETF-IP-FORWARDING-MIB
	• IP-MIB (was RFC2011-MIB)
	• TCP-MIB (RFC 2012)
	• UDP-MIB
	• CISCO-HSRP-EXT-MIB
	• CISCO-HSRP-MIB
	• CISCO-BGP-POLICY-ACCOUNTING-MIB
	QoS
	• MQC-MIB (Cisco Class-Based QoS MIB)
	• CISCO-PING-MIB
	Traps

	• RFC 1157
	• Authentication
	• Linkup
	• Linkdown
	• Coldstart
Gestión de redes	• Mejora de la CLI
	• Interfaz XML
	• Cisco CIT
	• Soporte SNMP y MIB
Energía	• Consumo máximo de energía cuando el chasis está totalmente configurado con tarjetas de línea con el tráfico de reproducción: 2551W
	• Fuente de alimentación del chasis Capacidad de salida máxima: 4 kW, tanto para la fuente de alimentación de CC y la fuente de alimentación de CA
Condiciones ambientales	Temperatura de almacenamiento: de -40 a 158 ° F (-40 a 70 ° C)
	Temperatura de funcionamiento:
	• Normal: 41 a 104 ° F (5 a 40 ° C)
	• A corto plazo: 23 a (-5 a 50 ° C) 122 ° F
	Humedad relativa:
	• Normal: 5 a 85 por ciento
	• Corto plazo: del 5 al 90 por ciento, pero que no exceda 0,024 kg de agua por kg de aire seco
	Nota: A corto plazo se refiere a un período de no más de 96 horas consecutivas y un total de no más de 15 días a 1 año. (Se refiere a un total de 360 horas en un año determinado, pero no más de 15 apariciones durante ese período de 1 año.)

Tabla 17.3.1. Especificaciones Básicas del equipo de Borde

CORE 7609-S CISCO	
Característica	
Versión software	Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 15.2(1)S2, RELEASE SOFTWARE (fc1)
Protocolos	CDP
	• IPv4 e IPv6
	• ICMP

	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• Multicast Source Discovery Protocol (MSDP)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• Protocolo de reserva de recursos (RSVP)
	• Servicios diferenciados (DiffServ) ingeniería de tráfico sea conscientes
	• plano de control MPLS Ingeniería de Tráfico (RFC 2702 y 2430)
	• Enrutamiento de Política Lingüística (RPL)
	• Gestión
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• Seguridad
	• Mensaje DigestAlgorithm 5 (MD5)
	• Protocolo (IPsec) de seguridad IP
	• Secure Shell Protocolo (SSHv2)
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
Tarjetas, puertos y ranuras	48 CEF720 48 port 1000mb SFP
	48 CEF720 48 port 1000mb SFP
	2 RouteSwitchProcessor 720 (Active)
	2 RouteSwitchProcessor 720 (Hot)
	0 4-subslot SPA Interface Processor-200
	48 CEF720 48 port 10/100/1000mb Ethernet
Memoria	40 Gb
Rendimiento	400 Mbps.
MIB QUE SOPORTA EL EQUIPO	sysUpTime.0
	interfaces
	ip
	ipForward
	ipTrafficStats

	mplsLsrStdMIB
	mplsLdpStdMIB
	ospf
	ospfTrap
	bgp
	dot1dBridge
	ifMIB
	nhrpMIB
	ipMRouteStdMIB
	igmpStdMIB
	pimMIB
	msdpMIB
	ciscoPingMIB
	ciscoIpSecFlowMonitorMIB
	ciscoIpSecPolMapMIB
	ciscoPimMIB
	ciscoBgp4MIB
	ciscoIfExtensionMIB
	ciscoEigrpMIB
	ciscoCefMIB
	ciscoBridgeDomainMIB
	ciscoNhrpExtMIB
	ciscoIpMRouteMIB
	ciscoIPsecMIB
	mplsLdpMIB
	cospf
	ciscoExperiment.101
	ciscoIetfIsisMIB
	ciscoIetfBfdMIB
	snmpTrapOID.0
	snmpMIB.1.4.3.0
	snmpTraps.3
	snmpTraps.4
Gestión de redes	• Mejora de la CLI
	• Interfaz XML
	• Cisco CIT
	• Soporte SNMP y MIB
Energía	-208 to 240 VAC (recommended)
	-48 to -60 VDC (4000 WAC supplies require 30A input circuits)

Condiciones ambientales	● Temperatura de funcionamiento : de 32 a 104 ° F (0 a 40 ° C)
	● Temperatura de almacenamiento : -40 a 167 ° F (-40 a 75 ° C)
	● Humedad rela□va: 10 a 90% , sin condensación
	● Cumplimiento de norma□vas

Tabla 1.7.3.2. Especificaciones Básicas del equipo de Core

DISTRIBUCIÓN 7613	
Característica	
Versión software	Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVENTERPRISEK9-M), Version 15.3(1)S, RELEASE SOFTWARE (fc1)
Protocolos	• Protocolo de descubrimiento de Cisco
	• IPv4 e IPv6
	• Protocolo de mensajes de control de Internet (ICMP)
	• Capa 3 protocolos de enrutamiento, incluyendo:
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• Protocolo de administración de grupos de Internet (IGMP) versiones 1, 2 y 3
	• multiprotocolo BGP (MBGP)
	• Multicast Source Discovery Protocol (MSDP)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• Protocolo de reserva de recursos (RSVP)
	• Servicios diferenciados (DiffServ) ingeniería de tráfico sea conscientes
	• plano de control MPLS Ingeniería de Tráfico (RFC 2702 y 2430)
	• GMPLS
	• Enrutamiento de Política Lingüística (RPL)
	• Gestión
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• Seguridad

	• Mensaje DigestAlgorithm 5 (MD5)
	• Protocolo (IPsec) de seguridad IP
	• Secure Shell Protocolo (SSHv2)
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
	• DHCP v6
	• EoMPLS
Memoria	40 GB
Rendimiento	720 Mbps
MIB QUE SOPORTA EL EQUIPO	sysUpTime.0
	interfaces
	ip
	ipForward
	ipTrafficStats
	mplsLsrStdMIB
	mplsLdpStdMIB
	ospf
	ospfTrap
	bgp
	dot1dBridge
	ifMIB
	nhrpMIB
	ipMRouteStdMIB
	igmpStdMIB
	ospfv3MIB
	pimMIB
	msdpMIB
	ciscoPingMIB
	ciscoIpSecFlowMonitorMIB
	ciscoIpSecPolMapMIB
	ciscoPimMIB
	ciscoBgp4MIB
	ciscoIfExtensionMIB
	ciscoEigrpMIB
	ciscoCefMIB
	ciscoBridgeDomainMIB
	ciscoNhrpExtMIB
	ciscoIpMRouteMIB
	ciscoIPsecMIB
	mplsLdpMIB

	cospf
	ciscoExperiment.101
	ciscoIetfIsisMIB
	ciscoIetfBfdMIB
	snmpTrapOID.0
	snmpMIB.1.4.3.0
	snmpTraps.3
	snmpTraps.4
Gestión de redes	CLI
	Interfaz XML
	• Cisco CIT
	• Soporte SNMP y MIB
Energía	Requisitos de Alimentación 208 to 240 VAC recomendado (or –48 to –60 VDC)
Condiciones ambientales	Temperatura de Almacenamiento: –4 to 149°F (–20 to 65°C)
	Temperatura de Operacion: 32 to 104°F (0 to 40°C)
	Humedad Operativo: 10 to 85%
	Humedad de Almacenamiento: 5 to 95%

Tabla 1.7.3.3. Especificaciones Básicas del equipo de Distribución

VSS		
Característica		
Versión software	Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(33)SXJ2, RELEASE SOFTWARE (fc4)	
Protocolos	IPv4 unicast forwarding, including MPLS VPN	Unidirectional Link Detection (UDLD)
	IPv4 multicast forwarding, including MPLS VPN	Gateway Load Balancing Protocol (GLBP)
	iBGP y eBGP	Hot Standby Routing Protocol (HSRP)
	OSPF	Virtual Router Redundancy Protocol(VRRP)
	EIGRP	UplinkFas
	RIPv1/v2	BackboneFast
	RIPv2	RSTP (802.1w)
	ISIS	PortFast
	Staticrouting	Per VLAN STP (PVSTP)

	Unidirectional link routing (UDLR)	Per VLAN RSTP (PVRSTP)
	IGMPv1, IGMPv2, IGMPv3	MultipleInstance STP (MISTP)
	PIMv1, PIMv2	MSTP (802.1s)
	SSM IGMPv3lite and URD	STP Root Guard
	Stub IP multicastrouting	L2VPN Advanced VPLS (A-VPLS)
	IGMP join	
	IGMP staticgroup	
	Multicastrouting monitor (MRM)	
	Multicast source discovery protocol (MSDP)	
	SSM	
	IPv4 Ping	
	IPv6 Ping	
	LAN Switching:	
	Layer 2 LAN Ports	
	Flex Links	
	EtherChannels	
	mLACP para Servidores de Acceso	
	IEEE 802.1ak MVRP and MRP	
	VLAN TrunkingProtocol (VTP)	
	VLANs	
	PrivateVLANs (PVLANs)	
	Private Hosts	
	IEEE 802.1Q Tunneling	
	Layer 2 ProtocolTunneling	
	STP and MST	
	MultiprotocolLabelSwitching (MPLS)	
	PROTOCOLOS QUE SE ENCUENTRAN CONFIGURADOS:	
	BGP ; AS:14420	
	IS-IS ; ID:1	

Tarjetas, puertos y ranuras	Puertos Gigabit Ethernet GBIC/SFP : 384. Configurado como Virtual SwitchingSystem: 768	
	Puertos 10 GBE XENPAK/X2: 130. Configurado como Virtual SwitchingSystem: 260	
	Puertos10/100/1000 Ethernet: 385. Configurado como Virtual SwitchingSystem: 770	
	Puertos 10 Gigabit Ethernet RJ-45: 128	
	Puertos 40 Gigabit Ethernet RJ-45: 32	
Memoria	40 GB	
Rendimiento	1.4 Tbps	
MIB QUE SOPORTA EL EQUIPO	ipForward	
	mplsLdpStdMIB	
	dot1dBridge	
	ciscoPingMIB	
	ciscoStpExtensionsMIB	
	ciscoIpSecFlowMonitorMIB	
	ciscoCat6kCrossbarMIB	
	ciscoEigrpMIB	
	ciscoIPsecMIB	
	mplsLdpMIB	
Gestión de redes	• CLI	
	• Interfaz XML	
	• Soporte SNMP y MIB	
Energía	• Cisco Catalyst 6509-V-E chassis soporta alimentación con fuentes AC y DC. Para Fuentes AC: 8700W.Para Fuentes DC: 4000W.	

	• La capacidad máxima de la fuente de alimentación es de hasta 14500W proporcionando la capacidad de soportar configuraciones completamente cargadas de corriente y futuras tarjetas 10 Ethernet Gigabit.	
Condiciones ambientales	Temperatura de almacenamiento: -4 to 149°F (-20 a 65°C)	
	Temperatura de funcionamiento: 32°F a 104°F (0 a 40°C)	
	Transición térmica: 0.5 ° C por minuto (caliente a frío) y 0. 33 ° C por minuto (frío a caliente)	
	Humedad relativa:	
	Ambiente (sin condensación) de funcionamiento: 5% a 90%	
	Ambiente (sin condensación) no operativos y de almacenamiento: 5% a 95%	

Tabla 1.7.3.4. Especificaciones Básicas del equipo VSS

ROUTE-REFLECTOR	
Característica	
Versión software	Cisco IOS XE Operating System, which is based on Cisco IOS Software Release 12.2SR
Protocolos	CDP
	• IPv4 e IPv6
	• ICMP
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• BGP
	• SNMPv3
	• PPPoX
	• DHCP
	• IPTV

	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
	• PPPoX
	• EIGRP
Tarjetas, puertos y ranuras	Management: 1 x 10Base-T/100Base-TX - RJ-45,
	Management: 1 x Console - RJ-45,
	Management: 1 x Auxiliary Input - RJ-45,
	LAN : 4 x SFP (mini-GBIC), USB : 1 x 4 pin USB Type A
Memoria	Instalada 4 GB Máxima hasta 8 GB
Rendimiento	1.8 gbps
MIB QUE SOPORTA EL EQUIPO	sysUpTime.0
	interfaces
	ip
	ipForward
	ipTrafficStats
	mplsLsrStdMIB
	mplsLdpStdMIB
	ospf
	ospfTrap
	bgp
	ifMIB
	nhrpMIB
	ipMRouteStdMIB
	igmpStdMIB
	pimMIB
	msdpMIB
	ciscoPingMIB
	ciscoIpSecFlowMonitorMIB
	ciscoIpSecPolMapMIB
	ciscoPimMIB
	ciscoBgp4MIB
	ciscoIfExtensionMIB
	ciscoEigrpMIB
	ciscoCefMIB
	ciscoNhrpExtMIB
	ciscoGdoiMIB

	ciscoIpMRouteMIB
	ciscoIPsecMIB
	mplsLdpMIB
	ciscoDlcSwitchMIB
	ciscoExperiment.101
	ciscoIetfIsisMIB
	ciscoIetfBfdMIB
	snmpTrapOID.0
	snmpMIB.1.4.3.0
	snmpTraps.3
	snmpTraps.4
Gestión de redes	● Telnet and Secure Shell (SSH) Protocol (command-line interface [CLI])
	● Console port (through the CLI)
	● Simple Network Management Protocol (SNMP)
	● RFC 2665
Energía	● Maximum (DC): 500W
	● Maximum (AC): 471W ● Maximum (out): 400W
Condiciones ambientales	Intervalo de temperatura operativa 0 - 40 °C
	Intervalo de temperatura de almacenaje -40 - 70 °C
	Intervalo de humedad relativa para funcionamiento 5 - 85 %
	Intervalo de humedad relativa durante almacenaje 5 - 95 %
	Altitud de funcionamiento -60 - 4000 m

Tabla 1.7.3.5. Especificaciones Básicas del equipo Route Reflector

1.8 REDUNDANCIA

El ISP de la CNT EP maneja redundancia a nivel de los equipos de comunicaciones de dos formas:

- REDUNDANCIA GEOGRAFICA: La estructura de capas y los equipos son el mismo modelo y marca de la Gráfica1.1 es decir en Guayaquil a nivel de tráfico y configuraciones soportan de la misma manera que en Quito.

- REDUNDANCIA LOCAL: El ISP mantiene redundancia local a nivel de equipos e interfaces, hay dos equipos VSS, Distribución, Route Reflector, Core cada uno de ellos maneja redundancia de conexiones físicas a nivel de interfaces y comparten la carga pero en el caso de algún incidente en alguno de ellos cualquiera puede soportar el tráfico total. Esta configuración lógica y Física se aplica también en Guayaquil.

A nivel LOCAL el equipo de Borde tiene redundancia de conexión de interfaces con los equipos Nube MPLS Internet.

2. CAPITULO II.- MARCO TEORICO

Las redes de telecomunicaciones continuamente se expanden, se vuelven complejas, heterogéneas por lo cual es necesario la gestión de su correcto funcionamiento y planificación de crecimiento.

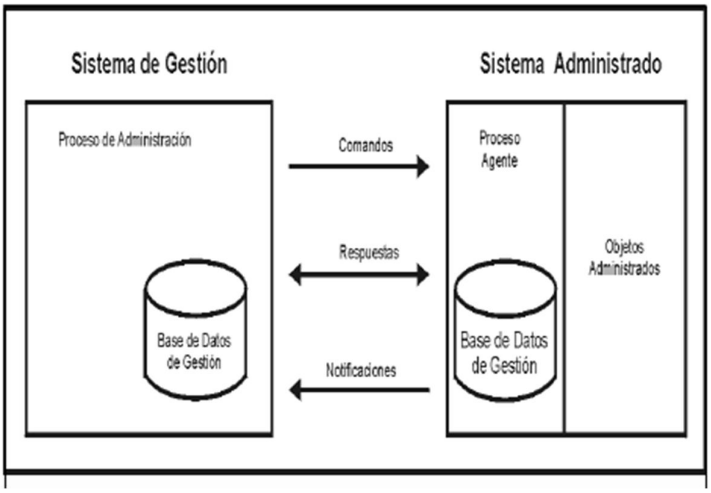
La Gestión de red son actividades dedicadas al seguimiento, control y monitoreo del equipamiento informático y de comunicaciones de la red de telecomunicaciones cuyo objetivo es garantizar un nivel de servicio de los recursos que se disponen.

Existen variedad de herramientas de gestión las cuales están basadas en el paradigma Gestor – Agente.

Un Gestor es el software que se encuentra en la central de gestión, responsable de iniciar-terminar la tarea de gestión.

Un Agente es el software que se encuentra en el dispositivo gestionado, interactúa con el gestor para atender las peticiones.

En la Gráfica2.1.1 que se muestra a continuación se detalla los componentes básicos de un Sistema de Gestión de Red.



Gráfica2.1.1. Componentes básicos de un sistema de Gestión de Red [1][8]

- Sistema de Gestión: Emite comandos, peticiones hacia el Sistema administrado.
- Agente: Emite respuestas, notificaciones hacia el gestor.
- Protocolo de Gestión: Controla las operaciones entre el sistema de gestión y el sistema administrado.
- Base de Datos de Gestión (MIB): almacena los datos de los objetos administrados del equipamiento informático y de comunicaciones de la red.

Los Sistemas de Gestión de Red es un conjunto de elementos informáticos, de comunicaciones y programas informáticos interconectados e interdependientes mediante los cuales se puede controlar, monitorear el estado y funcionamiento

[8]Referencia bibliográfica [1](EGAS, 2007)

global de la red de telecomunicaciones, están implementados a través de protocolos a nivel de aplicación.

2.1 ARQUITECTURA O MODELOS DE GESTION DE RED

2.1.1 Modelo de Gestion OSI (Open Systems Interconnection) [2]9

La Organización Internacional de Estándares ISO, estableció una arquitectura como modelo de referencia para el diseño de protocolos de Interconexión de Sistemas Abiertos conocido como OSI, a continuación un breve resumen de los siete niveles del Modelo OSI:

1) Nivel Físico: Se encarga de la conexión de los equipos al medio físico.
2) Nivel de Enlace: Detección, corrección de errores a nivel de la red, fragmenta y ordena en paquetes los datos enviados, realiza funciones básicas de control de flujo (evita congestión en el proceso de transmisión de datos).
3) Nivel de Red: Establecer, mantener y terminar conexiones entre sistemas proporcionando los medios adecuados. Principalmente permite direccionar los paquetes de datos que recibe del nivel de transporte.
4) Nivel de Transporte: Facilita la transferencia de datos entre nodos finales, proporciona integridad de los mismos.

[9] Referencia bibliográfica [2] (Subramanian, 2012)

5) Nivel de Sesión: Establecer, gestionar y terminar sesiones entre aplicaciones.
6) Nivel de Presentación: Encargada de la representación de los datos, los datos llegan de manera reconocible a pesar de que diferentes equipos tengan diferentes representaciones internas de caracteres, sonido o imágenes.
7) Nivel de Aplicación: también conocida "nivel de usuario", es el destino final de los datos donde se proporciona los servicios al usuario.

Este modelo provee el estándar para la comunicación entre sistemas informáticos a través de una red utilizando protocolos a nivel de aplicación para intercambio de información entre el agente y el gestor. Esta arquitectura maneja una interfaz entre los dispositivos que ofrecen funciones de gestión la cual la denomina objeto gestionado. Un objeto gestionado trabaja con los atributos que son las propiedades del objeto y el comportamiento de las respuestas a las operaciones solicitadas.

En la arquitectura ISO se describe cada objeto gestionado en cuatro propiedades:

- Atributos: corresponden a las características de un objeto, éstas son reconocidas en su interfaz.
- Operaciones: son las operaciones (escritura, lectura y configuración) que

están a cargo de un objeto.

- Notificaciones: son los reportes que el objeto puede generar.
- Comportamiento: son las respuestas del objeto sobre las operaciones realizadas sobre éste.

Para establecer la comunicación entre el gestor y el objeto gestionable interviene el agente de gestión. El protocolo Común de Información de Gestión (CMIP, Common Management Information Protocol) se encarga de establecer el flujo normal de información de gestión entre el gestor y el agente permitiendo que un sistema se pueda configurar para que opere como gestor o agente.

2.1.1.1 Áreas funcionales del modelo de gestion osi

De acuerdo a la Organización Internacional de Estándares (ISO, International Standard Organization), las áreas funcionales de la Gestión de la Red abarcan 5 grupos: [1][10]

1) Gestión de Fallos y Recuperación
2) Gestión de la Configuración
3) Gestión del Rendimiento
4) Gestión de la Contabilidad

[10]Referencia bibliográfica [1](EGAS, 2007)

5) Gestion de la Seguridad

El alcance de este proyecto es trabajar sobre el modelo de Gestión de Fallas por lo cual a continuación se realizará una breve descripción del mismo.

1) Gestión de Fallos y Recuperación

La Gestión de Fallas son un conjunto de actividades que permiten la detección de la ocurrencia de falla, el aislamiento de la causa de la falla y la corrección de la misma que pudiesen ocurrir en las redes o sistemas de comunicaciones permitiendo mantener activamente el nivel de servicio de la red.

Gestión de Fallas se encarga de las siguientes tareas:

- Supervisión de alarmas
- Localización de Fallas
- Corrección de Fallas

La gestión de fallos busca una gestión proactiva en la cual la detección de fallos sea realizada antes de que suceda. También busca evitar fallas determinando mediante tendencias o umbrales monitoreo que permitan anticipar la falla.

Las funciones principales de Gestión de Fallas son:

1. Supervisión del estado de la red: mediante herramienta de monitoreo.
2. Detección de problemas: mantenimiento preventivo.
3. Respaldo de configuración: generación de respaldos puede ser automático o manual.
4. Diagnóstico y Reparación: mantenimiento correctivo.

2.1.2 Modelo de Gestión TMN (Telecomunications Management Network)

Acogiendo el modelo Gestor Agente de OSI, el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones establece el modelo Red de Gestión de Telecomunicaciones (TMN) el cual está definido en la recomendación M.3010 (Principios para una red de gestión de las telecomunicaciones) y el CCITT (Comité Consultivo Internacional para Telefonía y Telegrafía).

El modelo TMN está orientado a proveer una estructura estándar de red con lo que desea interconectar diversos tipos de sistemas de operación y equipos de telecomunicaciones.

Arquitecturas que se manejan en TMN: [1][11]

- Arquitectura Funcional: se basa en bloques funcionales.
    - Bloque Funcional de sistema de Operación (Operations System Function, OSF). Funciones del Gestor.
    - Bloque Funcional de Estación de Trabajo (Work Sattion Function, WFS). Interfaz entre el usuario con el sistema de operaciones.
    - Bloque Funcional de Adaptador Q (Q Adaptor Function, QAF). Permite gestionar elementos de red con sistema de gestión propietario.
    - Bloque Funcional de Mediación (Mediation Function, MD). Opera sobre la información que llega al NEF de los QAF para adecuarla al formato usado por OSF.

TMN también define arquitecturas para identificar la información transmitida entre los bloques funcionales y de detallan a continuación:

- Arquitectura Física: el propósito es que los bloques funcionales se implementen en equipos físicos interconectados entre sí a través de interfaces.

[11]Referencia bibliográfica [1](EGAS, 2007)

- Arquitectura de Información de TMN. La información que se trasmite entre los bloques funcionales la define mediante un formato.
- Arquitectura Organizativa de TMN define jerarquías entre gestores, bajo nivel los que están orientados a problemas técnicos de los recursos y gestores de alto nivel orientados a garantizar la calidad del servicio.

2.1.3 Modelo de Gestión de Internet

La Fuerza de trabajo de Ingeniería del Internet (IETF, Internet Engineering Task Force) es el organismo encargado de la estandarización de la Gestión Internet.

2.1.3.1 Arquitectura de gestión de red en internet

El protocolo estándar para la conexión en Internet es TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet), el cual es usado para que equipos que no pertenecen a una misma red pueden operar servicios como Telnet, FTP, correo electrónico y otros.

El protocolo TCP/IP está confirmado por:

- El **Protocolo de Control de Transmisión (TCP)** permite establecer conexiones e intercambiar datos entre elementos de la red garantizando la entrega de

los mismos en el mismo orden en el cual fueron enviados.

- El **Protocolo de Internet (IP)** permite la interconexión de redes de comunicación entre elementos de la red basado en el método de envío de datos o conmutación de paquetes utilizando direcciones IP.

El protocolo de control de mensajes de Internet (ICMP) fue originalmente el protocolo de gestión de red en Internet, debido al incremento de elementos de la red (switch, routers, etc) se volvió una necesidad el desarrollar nuevos protocolos de gestión y ahí se crea el protocolo de gestión SNMP.

La arquitectura de red en Internet entonces trabaja con el protocolo de administración simple de red (SNMP) el cual a su vez está estructurado de la siguiente manera: [3][12]

- Estructura de administración de información (SMI): definido por el RFC 1155 la cual se encarga de la estructura e identificación de información de Gestión para redes basadas en TCP/IP, considerada como la gramática para escribir MIB de SNMP.
- Base de Información de Administración (MIB): definida por la RFC 1212 el cual especifica un formato para la producción de los módulos MIB, almacena

[12]Referencia bibliográfica [3] (SNMP, 2015)

información de los objetos que están organizados de forma jerárquica y accedidos a través del protocolo SNMP.

- Protocolo de administración simple de red (SNMP): definido por la RFC 1157 por el cual la información de gestión entre las estaciones de gestión de red y los agentes en los elementos de red puede ser inspeccionada lógicamente y de manera remota.

A continuación se detalla los modelos que despliega la arquitectura SNPM:

- Modelo de Información de gestión de Internet:
    - SMI: estructura de la información, organización de objetos.
    - MIB: información de gestión almacenada en los agentes.
    - ASN.1.: Notación, definición de la información de la MIB.

        - ASN.1.: define el formato PDU SNMP (Tipos de datos por ejemplo: counter, Valores por ejemplo: ifTable y Macros por ejemplo: OBJECT-TYPE, ACCES).

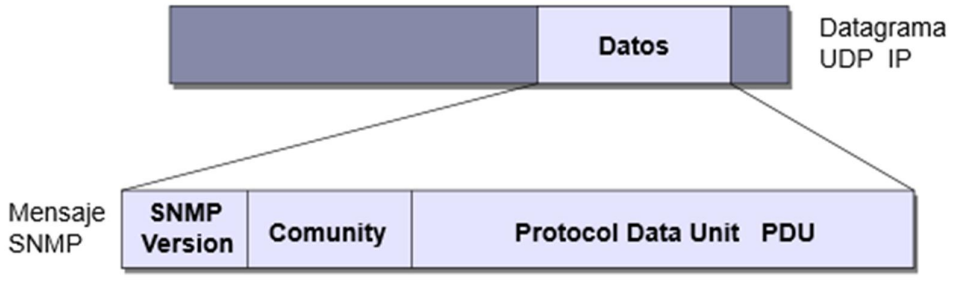
- Modelo de Comunicaciones de gestión de Internet: SNMP emplea User Datagram Protocol (UDP) el cual realiza el transporte no orientado a la conexión, es decir no trabaja con acuses de recibo para garantizar la

entrega, no ordena los paquetes ni existe control de flujo.

2.1.3.1.1 Simple Network Management Protocol (SNMP)

Es importante conocer la relación que existe a nivel de SNMP y el Modelo OSI, la capa aplicación del modelo OSI está orientada al destino final de los datos donde se proporciona los servicios al usuario; SNMP es un protocolo que permite al usuario SNMP interactuar sobre los objetos de un dispositivo a través de un Agente SNMP entendiéndose así como un modelo de comunicación cliente o usuario – Servidor o Agente.

Por otra parte también es necesario conocer cómo trabaja el mensaje SNMP como se puede observar en la Gráfica2.1.3.1.1:



Gráfica2.1.3.1.1. Mensaje SNMP [4][13]

En donde los componentes especifican:

[13] Referencia bibliográfica [4](MOLERO, 2010)

- Versión: Protocolo SNMP, v.1, v.2, ó v.3.
- Comunity: o Comunidad el cual es el identificativo para autenticación controlando el acceso de un dispositivo.
- Protocol Data Unit (PDU): contiene el cuerpo del mensaje SNMP. PDU más comunes: GetRequest, GetResponse, SetRequest.
    - GetRequest: Consulta el valor o estado de un objeto dentro del dispositivo.
    - GetResponse: respuesta a un Request con el valor o estado de un objeto.
    - SetRequest: modifica el valor de un objeto dentro del dispositivo, después de esta modificación el Agente SNMP confirma la operación con un GetResponse.

Los mensajes SNMP manejan operaciones de lectura (GET, GETNEXT, GETBULK), escritura (SET) y notificaciones (TRAP: alerta al administrador ante un evento sucedido en el dispositivo como routers, switches, servidores).

Las mejoras en la versión SNMP v2 son los formatos de mensaje traps, se adiciona PDU de GetBulk e Inform, la primera recupera grandes bloques de datos, y la segunda permite enviar traps de información entre NMS cuando haya recibido una

respuesta respectivamente.

La versión SNMP v3 proporciona acceso seguro a los dispositivos mediante autenticación y encriptación de los paquetes a través de la red es decir maneja seguridades basado en la RFC 3410.

2.1.3.1.2 Base de información de gestión "MIB"

La Base de Información de Gestión (MIB), se define como una base de información virtual que recopila Objetos los cuales se encuentran organizados en base a un conjunto de reglas, que modelan la información en el campo de la sintaxis y la semántica es decir manejan una correlación de numéricos a nombres legibles. Los objetos se encuentran como hojas de los nodos o ramas desprendidos de una raíz. La raíz no está provista de etiquetas ni numeración, los nodos sí se identifican en forma legible por medio de etiquetas.

En la Figura 2.1.3.1.2.1 se muestra la información del el árbol MIB, y el grupo identificado con el nombre interfaces.

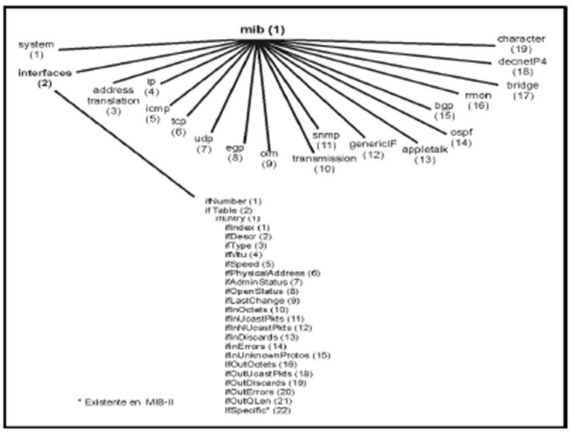


Figura 2.1.3.1.2.1 Información Grupos MIB-Interfaces SNMP [1][14]

Las MIB son variables definidas por expertos para cada una de las tecnologías o recursos que forma la red, los fabricantes también pueden adicionar variables específicas de su producto en nuevas definiciones de MIB.

Para que los fabricantes puedan adicionar las variables en MIB deben disponer de un OID asignado por alguna de las agencias registradoras existentes como son la IANA, ANSI o BSI.

Un OID, o Identificador de Objeto, es una secuencia de números que se asignan jerárquicamente y permite identificar objetos en la red.

En la Figura1 se muestra un ejemplo de la jerarquía de la MIB empezando desde la raíz, luego los nodos y luego los subnodos.

[14]Referencia bibliográfica [1] (EGAS, 2007)

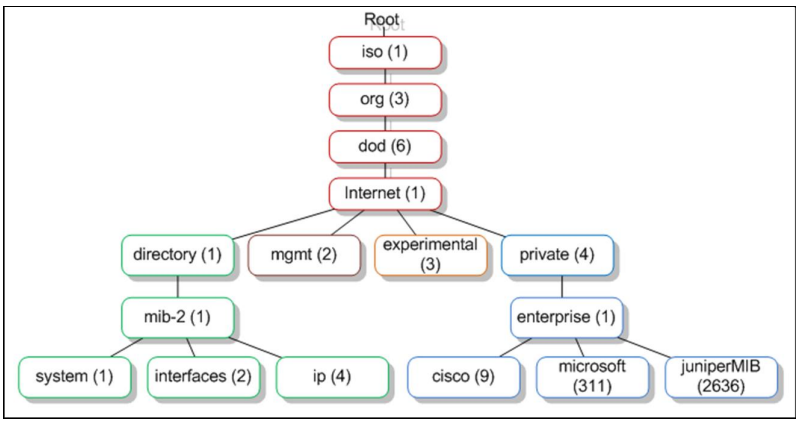


Figura2.1.3.1.2.2. Ejemplo de un árbol MIB [4][15]

De acuerdo a la Figura2.1.3.1.2.2 la raíz contiene los siguientes nodos, y su valor equivalente:

iso = 1

org = 3

dod = 6

Internet =1

Debido a que el nodo de interés de este proyecto es Internet, a continuación se detalla una breve explicación de los campos que contiene:

- directory (1): directorio OSI

[15]Referencia bibliográfica [4] (MOLERO, 2010)

- mgmt (2) : objetos estándares RFC
- expemimental (3): experimentos Internet
- private (4): Específico a los vendedores

Dentro de private se encuentra otro subnodo que hace referencia a enterprise que significa empresa, de esta rama cuelgan las empresas que han adicionado variables específicas de su producto en nuevas definiciones de MIB.

En la Figura2.1.3.1.2.2 se verifica que el OID asignado para CISCO es 9 entonces las MIB de CISCO serán identificadas de acuerdo al siguiente OID: 1.3.6.1.4.1.9.

Para los casos en los cuales requerimos trabajar con los OIDs estándares podemos observar en la Figura2.1.3.1.2.3 los objetos que corresponden al grupo interfaces.

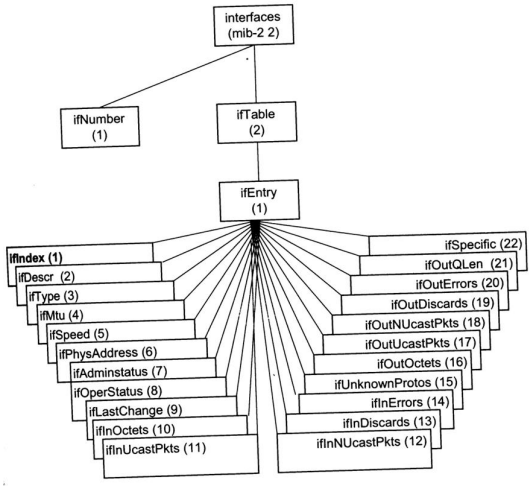


Figura2.1.3.1.2.3. Objetos del grupo interfaces. [2][16]

[16] Referencia bibliográfica [1] (Subramanian, 2012)

De acuerdo a la Figura2.1.3.1.2.2 y Figura2.1.3.1.2.3 el objeto del grupo de interfaces se identifica de la siguiente manera:

OID=1.3.6.1.1.1.1.2.2.1.8 y su objeto es ifOperStatus.

En la Tabla2.1.3.1.2.1 se detalla los grupos MIB que pueden ser gestionados en INTERNET por SNMP.

GRUPOS MIB A SER GESTIONADOS EN INTERNET POR SNMP	
SISTEMA	Información específica del objeto como hardware, software, versión, localización física, etc.
INTERFACES	Interfaces por las que los nodos pueden enviar / recibir paquetes de datos.
TRADUCCION DE DIRECCIONES	Tablas para mapear direcciones de red (IP) a direcciones físicas (MAC).
IP	Tablas que tienen información de paquetes de datos enviados, recibidos.
ICMP	Estadísticas de entrada y salida del mensaje de Internet Control Message Protocol
TCP	Número máximo de conexiones TCP que puede soportar un objeto
UDP	Provee estadísticas de tráfico UDP. Detalles sobre datagramas UDP
EGP	Estadisticas de configuración de las funciones EGP (External Gateway Protocol) soportadas.
TRANSMISION	Información sobre el medio de transmisión.
SNMP	Información del agente SNMP, número de paquetes SNMP recibidos etc gestionado a través de una base de datos MIB

Tabla2.1.3.1.2.1. Grupos MIB gestionados por SNMP en Internet [5][17]

[17] Referencia bibliográfica [5] (COMER, 2014)

2.2 HERRAMIENTAS DE MONITOREO DE RED O AGENTES SNMP

Una herramienta de monitoreo de red o agente SNMP es un programa de interfaz de gestión de red, que interactúa con aplicaciones de gestión SNMP a través de sus atributos; realiza peticiones para recuperar datos y crear atributos de gestión. El agente SNMP se comunica con una aplicación de gestión SNMP usando el protocolo UDP permitiendo éste al agente SNMP y a la aplicación de gestión SNMP habitar en la misma máquina o en diferentes.

En la actualidad existen varias herramientas de monitoreo de red o Agentes SNMP unos de código abierto o software libre como Nagios, Zabbix, Cacti, Zenoss, y otras de software licenciado con costo como PRTG. En CNT EP se trabaja con las herramientas de monitoreo de Red PRTG y CACTI.

2.2.1 Comparación entre herramientas de monitoreo CACTI vs PRTG.

A continuación se realiza una comparación entre las herramientas CACTI y PRTG, en la Tabla2.2.1.1 se puede observar las semejanzas que maneja cada herramienta.

SEMEJANZAS		
CARACTERÍSTICA	**CACTI**	**PRTG**
Protocolo SNMP	SI	SI
Syslog	SI	SI
Alarmas (umbrales)	SI	SI
Weathermap	SI	NO

Tabla2.2.1.1 Semejanzas

En la Tabla2.2.1.2 se puede observar las diferencias entre las herramientas de monitoreo CACTI y PRTG.

DIFERENCIAS		
CARACTERÍSTICA	**CACTI**	**PRTG**
Autodescubrimiento	SI	SI
Método de data storage	RRDtool, MySQL	Propietario
Licencia	GPL	Pruebas / Comercial
Recolección de datos	SNMP, RRD Tool	Más de 200 sensores (PING,HTTP, SMTP,POP3, SNMP,FTP, WMI)
Análisis de tipo de tráfico	NO	SI sniffer, netflow
Generación de reportes	Requiere plugin	SI

Tabla2.2.1.2 Diferencias

PRTG brinda las mismas características que CACTI y otras adicionales, como mayor número de sensores para recolección de datos, generación de reportes, monitorización de ancho de banda vía netflow y sniffers. Adicionalmente PRTG al ser un sistema comercial brinda mantenimiento y actualización de software, soporte en línea.

Una gran desventaja que tiene PRTG es que no permite disponer de gráficos de mapas en línea que muestran la arquitectura de la red, sin embargo se puede tener en línea el consumo de ancho de banda de una interfaz.

CACTI es una herramienta web de monitoreo de red de software libre o código

abierto, busca automáticamente todas las interfaces de un dispositivo, está diseñada con interfaz gráfica y maneja los data de RRDtool, se puede visualizar el monitoreo en tiempo real del estado de las interfaces, utilización de ancho de banda de red, el tráfico de red etc.

Es muy útil para disponer de gráficos en línea que muestran la arquitectura de la red, el consumo de ancho de banda de una interfaz. Sin embargo no permite correlacionar errores.

La gran ventaja de CACTI es que permite una visualización gráfica de la red de una manera rápida y cómoda, es muy fácil consultar el estado mediante la visión de las gráficas correspondientes a cada nodo y segmento de equipos dentro del mismo. Estos mapas son conocidos como WEATHERMAP.

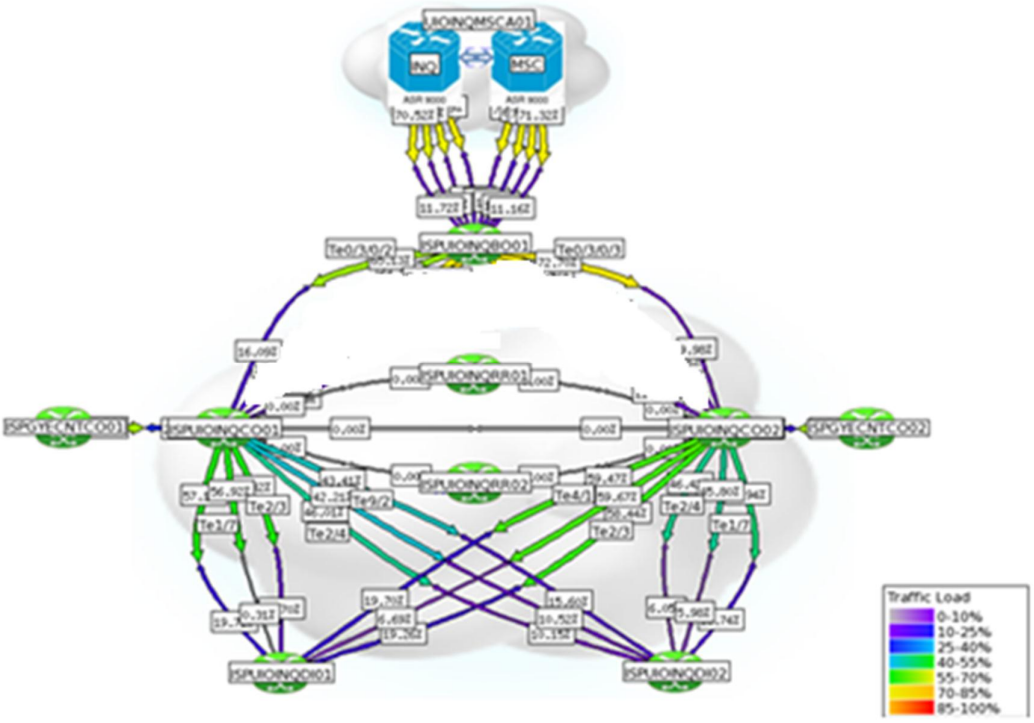


Figura2.2.0 Visualización gráfica de la red de ISP en Guayaquil [6]18

Como se puede observar en la Figura2.2.0, muestra la ingeniería en forma de mapa de la red del ISP en la ciudad de Guayaquil, se encuentra graficado los equipos que componen esta red, la interconexión entre equipos mediante interfaces, la capacidad de cada una de las interfaces, el estado de ocupación de las mismas, el estado físico, de esta manera facilita la gestión de administración de fallas a nivel del equipamiento del ISP por esa razón es considerada esta herramienta para trabajar en el objeto de este proyecto.

[18] Referencia bibliográfica [6] (CACTI, 2015)

2.2.2 Herramienta de monitoreo de Red CACTI

CACTI es la principal herramienta utilizada en el ISP de CNT para el monitoreo de la red de comunicaciones, monitoreo de enlaces de clientes corporativos los cuales mantienen un SLA suscrito. Permite visualizar de manera gráfica la arquitectura de red de comunicaciones que se encuentra implementada, debido a que es un software libre permite mediante generación de scripts personalizar los monitoreo, con un estudio más a fondo de este aplicativo se puede levantar scripts que permitan obtener información de los dispositivos no solo mediante SNMP si no también SSH y otros métodos. Por lo expuesto se utilizará esta herramienta para la obtención de los principales indicadores de falla de la red de comunicaciones del ISP.

A continuación se presenta una breve descripción de CACTI, sus principales características y modo de operación.

Cacti es una solución de software libre basada en RRDtool, desarrollada con PHP permite la generación de gráficos en red, visualizar las gráficas mediante la web, simplifica la administración de una red debido a que permite ver el estado de los

equipos que integran la red, los datos de RRDtool se almacenan en una base de datos MySQL. [9][19].

Al ser un sistema de software libre dentro de sus manuales de instalación indica los requisitos mínimos a nivel de software instalado (tomado de pdf: The Cacti Manual, published 2012, copyright@2012 the Cacti Group):

Requerimientos de SOFTWARE

- RRDtool 1.0.49 o 1.2.x
- MySQL 4.1.x o 5.x
- PHP 4.3.6 o superior, 5.x es recomendable las versiones recientes
- Un servidor Web, Apache o IIS

Requerimientos de HARWARE

Servidor Virtual:

Procesador	4 virtualCPUs
Memoria	4 GB
Disco Duro	24 GB

Servidor Físico:

Procesador	2 Procesadores
Memoria	32 GB
Disco Duro	Total 1 TB se encuentra en (Raid 1 ï Volume Group 500 GB)

[19] Referencia bibliográfica [9] (CACTI, 2015)

Requerimientos en los equipos a ser monitoreados:

- CACTI usa SNMP para recopilar información de los equipos a ser monitoreados, por tal razón es un agente y los elementos deben tener cargado el cliente SNMP v1, v2 o v3 y permitir el acceso al agente SNMP.

En base a lo indicado anteriormente, una vez instalado el software libre CACTI y haber ingresado al menú principal se mostrará una pantalla que se puede observar en la Figura 2.2.1.

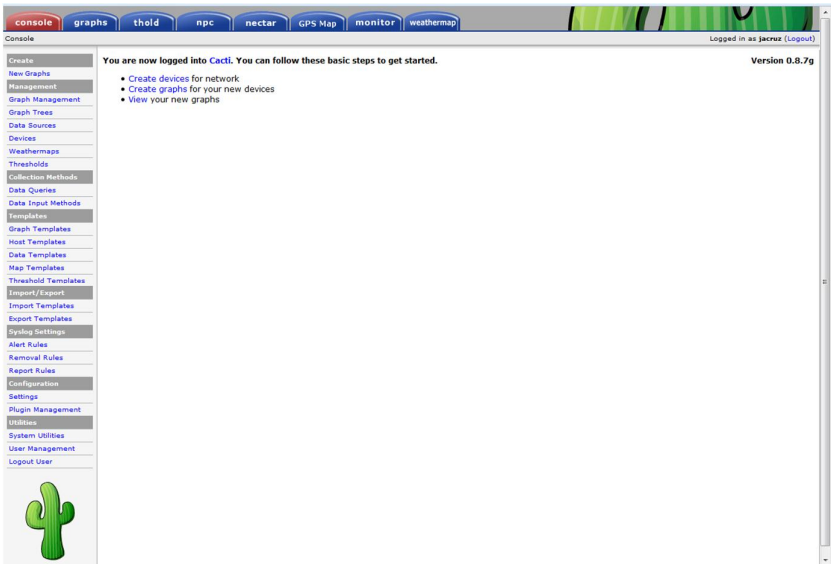


Figura 2.2.1 Primera pantalla de ingreso a CACTI [6]20

[20] Referencia bibliográfica [6] (CACTI, 2015) de aquí en adelante las gráficas de CACTI que se muestran corresponden a esta referencia bibliográfica.

CACTI está conformado por un RRDtool, PHP, MySQL, soporta SNMP y trabajan con una interfaz gráfica. Usa RRDtool para crear gráficos para cada equipo o elemento, los datos de RRDtool se guardan en la base de datos MySQL.

CACTI realiza la colección de datos vía SNMP, éstos pueden ser actualizados mediante SNMP o SCRIPTS. Permite la creación de plantillas para ser utilizadas el momento de agregar otro equipo.

CACTI permite monitorear una red IP mediante Creación de Gráficas y Alarmas, presenta los resultados de los monitores tipo árbol y de manera gráfica como se muestra en la Figura 2.2.2.

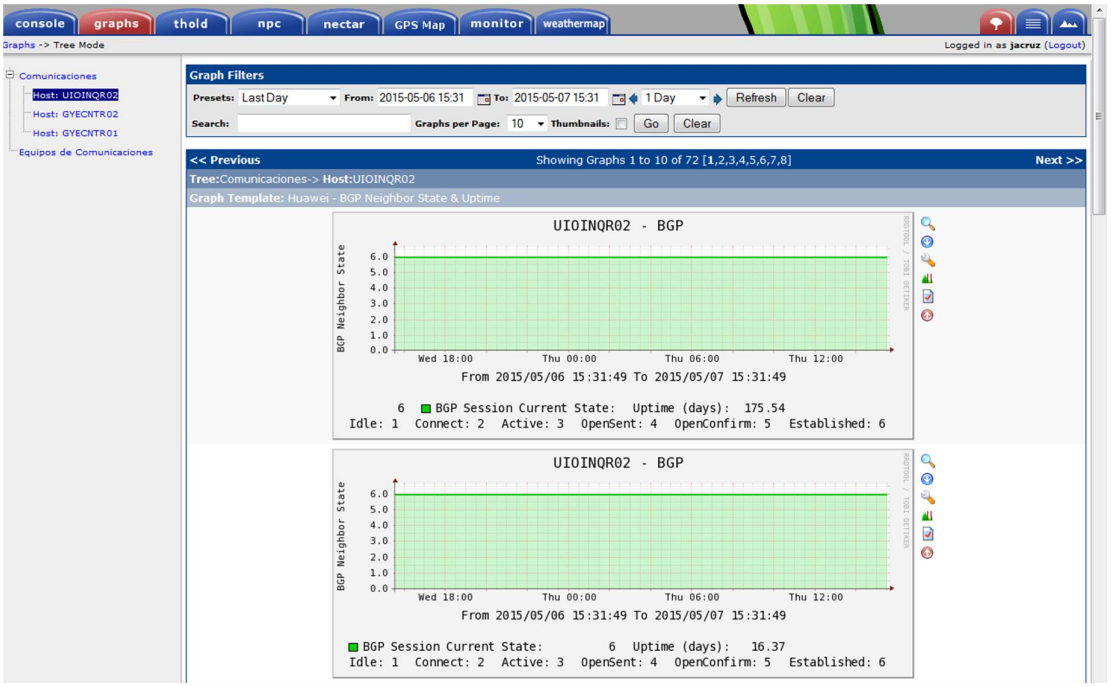


Figura 2.2.2 Presentación de monitoreo CACTI

Las gráficas del CACTI se crean utilizando datos recolectados vía SNMP. Una manera de recolectar estos datos es con los Data Queries, los cuales obtienen información indexada de un equipo.

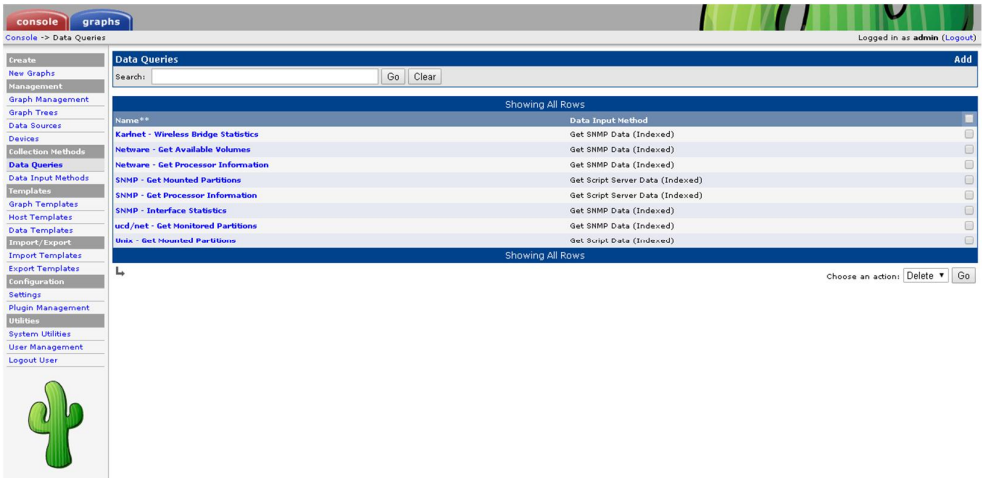


Figura 2.2.3 Data Queries por defautl

En la Figura 2.2.3 se puede observar los Data Queries que son cargados por defecto el momento de instalar CACTI.

En la Figura 2.2.4 se puede observar los Data Queries que obtuvo de un equipo en este caso el de Borde de Guayaquil, la lista es inmensa por esa razón se ha realizado el corte de la gráfica.

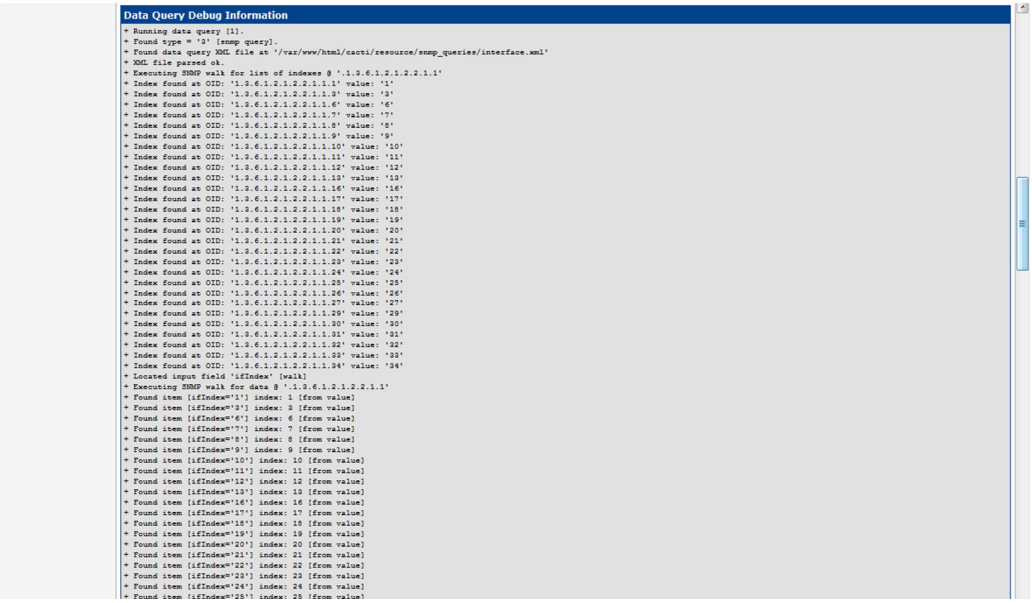


Figura 2.2.4 Data Queries Information

En la Figura 2.2.5 se puede observar el Data Querie SNMP obtenido específicamente para las interfaces estáticas del equipo de Borde de Guayaquil.

Data Query [SNMP - Interface Statistics]

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	HSpeed	Hardware Address
1	Down	MgmtEth0/RP0 /CPU0/0	MgmtEth0/RP0 /CPU0/0		ethernetCsmacd(6)	10000000	10	64:00:F1:03:1C:EA
3	Up	Null0	Null0		other(1)	0	0	
6	Up	TenGigE0/0/0/0	TenGigE0/0/0/0	### Te0/0/0/0 - LINK TO ISPGYECNTCO01 - Te1/1 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:29
7	Up	TenGigE0/0/0/1	TenGigE0/0/0/1	### Te0/0/0/1 - LINK TO C-GYEBLLCNTA01-BLL TE 1/1/1/2 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:2A
8	Up	TenGigE0/0/0/2	TenGigE0/0/0/2	### Te0/0/0/2 - LINK TO ISPGYECNTCO02 - Te2/3 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:2B
9	Up	TenGigE0/0/0/3	TenGigE0/0/0/3	### Te0/0/0/3 - LINK TO C-GYEBLLCNTA01-BLL TE 1/0/1/2 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:2C
10	Up	TenGigE0/1/0/0	TenGigE0/1/0/0	### Te0/1/0/0 - LINK TO ISPGYECNTCO02 - Te1/1 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:76
11	Up	TenGigE0/1/0/1	TenGigE0/1/0/1	### Te0/1/0/1 - LINK TO C-GYEBLLCNTA01-CNT TE 0/0/1/2 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:77
12	Up	TenGigE0/1/0/2	TenGigE0/1/0/2	### Te0/1/0/2 - LINK TO ISPGYECNTCO01 - Te2/3 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:78
13	Up	TenGigE0/1/0/3	TenGigE0/1/0/3	### Te0/1/0/3 - LINK TO C-GYEBLLCNTA01-CNT TE 0/1/1/2 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:79
16	Down	MgmtEth0/RP1 /CPU0/0	MgmtEth0/RP1 /CPU0/0		ethernetCsmacd(6)	10000000	10	64:00:F1:03:1C:E6
17	Up	Loopback100	Loopback100	### Lo100 - LOOPBACK IBGP ###	softwareLoopback(24)	0	0	
18	Up	Loopback101	Loopback101	### Lo101 - LOOPBACK IBGP-IPV6 ###	softwareLoopback(24)	0	0	
19	Up	Loopback102	Loopback102	### Lo102 - LOOPBACK EBGP ###	softwareLoopback(24)	0	0	
20	Up	Loopback103	Loopback103	### Lo103 - LOOPBACK EBGP-IPV6 ###	softwareLoopback(24)	0	0	
21	Up	ServiceInfra1	ServiceInfra1		other(1)	1024000	1	
22	Up	ServiceApp41	ServiceApp41	****INTERFACE IPV4 6rd*****	other(1)	4294967295	20480	
23	Up	ServiceApp61	ServiceApp61	****INTERFACE IPV6 6rd*****	other(1)	4294967295	20480	
24	Up	Loopback666	Loopback666	***testcgn***	softwareLoopback(24)	0	0	
25	Up	ServiceApp42	ServiceApp42	****INTERFACE IPV4 6rd*****	other(1)	4294967295	20480	
26	Up	ServiceApp62	ServiceApp62	****INTERFACE IPV6 6rd*****	other(1)	4294967295	20480	
27	Up	Bundle-Ether12	Bundle-Ether12	**** ETHERCHANNEL A C-GYEBLLCNTA01 ****	propVirtual(53)	4294967295	60000	28:94:0F:19:40:03
29	Up	TenGigE0/2/0/0	TenGigE0/2/0/0	### Te0/2/0/0 - LINK TO C-GYEBLLCNTA01-BLL TE 1/7/1/0 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:C3
30	Up	TenGigE0/2/0/1	TenGigE0/2/0/1	### Te0/2/0/1 - LINK TO C-GYEBLLCNTA01-CNT TE 0/7/1/2 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:C4
31	Up	TenGigE0/2/0/2	TenGigE0/2/0/2	### Te0/2/0/2 - LINK TO ISPGYECNTCO01 - Te7/1 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:C5
32	Up	TenGigE0/2/0/3	TenGigE0/2/0/3	### Te0/2/0/3 - LINK TO ISPGYECNTCO02 - Te7/1 ###	ethernetCsmacd(6)	4294967295	10000	28:94:0F:19:43:C6
33	Up	ServiceApp44	ServiceApp44	## NAT44 INSIDE PRIVADO ##	other(1)	4294967295	20480	

Figura 2.2.5 Data SNMP Interface Statistics

Los Graph Templates también sirven para generar gráficas sin embargo no recolectan información indexada directamente; pero pueden consultar valores de OIDs específicos en un equipo, es decir podemos colocar en la plantilla del template el valor de OID que deseo sea monitoreado no es auto descubierto por defecto.

Figura 2.2.5 Graph Templates

Cuando genera un autodescubrimiento por SNMP de un equipo arroja información del sistema, software, Uptime, Hostname, Localización y contacto, como se muestra en la Figura 2.2.6.

Figura 2.2.6 Información SNM extraída de un equipo

En CACTI para que un equipo sea graficado se debe agregar los Graph Templates y Data Queries. Es importante conocer que cuando se agrega alguna configuración en

el equipo, se debe realizar un redescubrimiento de los datos SNMP, para que la información se actualice en el CACTI.

2.2.3 Herramienta de monitoreo de Red CACTI y Modelo de Gestión de Internet (SNMP)

Como se había explicado anteriormente hay varias arquitecturas o modelos de gestión de red como es el modelo de Gestión en sistemas OSI, este modelo provee el estándar para la comunicación entre sistemas informáticos a través de una red utilizando protocolos a nivel de aplicación para intercambio de información entre el agente y el gestor, esto es posible con una interfaz entre los dispositivos que ofrecen funciones de gestión la cual la denomina objeto gestionado. Un objeto gestionado trabaja con los atributos que son las propiedades del objeto y el comportamiento de las respuestas a las operaciones solicitadas. El modelo de gestión en sistemas OSI trabaja con áreas funcionales como gestión de fallas, configuración, rendimiento, contabilidad, seguridad. Otro modelo de Gestión es el TMN el cual está orientado a proveer una estructura estándar de red con lo que desea interconectar diversos tipos de sistemas de operación y equipos de telecomunicaciones.

Por último hablamos sobre el Modelo de Gestión de Internet, mismo que trabaja

con el protocolo de administración simple de red (SNMP). Este protocolo trabaja a través de comunidades definidas las cuales permiten la comunicación del gestor SNMP gestor y el agente SNMP.

SNMP es el protocolo de gestión de red más usado en la actualidad, está definida en la capa de Aplicación para consulta a los diferentes elementos que forma una red como son los routers, switches, hosts, módems etc.

El modelo de gestión de Internet es el objeto de este trabajo ya que el ISP es un proveedor de servicios de Internet, el protocolo que trabaja en internet es SNMP y en este proyecto se trabaja en los equipos de comunicaciones de ISP.

2.3 REVISIÓN Y OBTENCIÓN DE LOS PRINCIPALES INDICADORES POR EQUIPO

De acuerdo a lo indicado en el capítulo I de este proyecto, los equipos de la Red de comunicaciones del ISP sobre los cuales obtendré los principales indicadores de falla son los denominados: BORDE, CORE y DISTRIBUCION.

Los equipos routers Route Reflector o Reflector de Ruta como se describió en el capítulo I permiten la configuración de concentrar el enrutamiento IBGP y direccionar a los equipos vecinos las tablas de enrutamientos de manera

automática, por tanto estos equipos al no cursar tráfico de red no forman parte del análisis de los indicadores de fallas.

Los equipos switchs denominados Virtual Switch que operan en la capa del Core encargados de la interconexión en capa 2 de los servicios que brindan valor agregado del ISP, tampoco serán analizados en este proyecto.

En CACTI se puede instalar un plugin para recolectar información sobre tráfico IP (NetFlow) y se debe implementar esta función en los equipos cisco sin embargo de las experiencias obtenidas en pruebas realizadas anteriormente, esta función incrementa la carga del CPU pudiendo ocasionar que los equipos dejen de operar por esa razón se encuentra deshabilitada esta opción y no será analizada.

Para obtener las MIBs que relacionen los indicadores de gestión de fallas lo podemos realizar de las siguientes maneras:

a. Podemos consultar en CISCO cuales son las MIBs de cada equipo:

Ingresar a la url: http://tools.cisco.com/ITDIT/MIBS/MainServlet., colocar la versión del reléase de software, el modelo o familia CISCO a la que pertenece el equipo, las principales funciones y realizar la búsqueda.

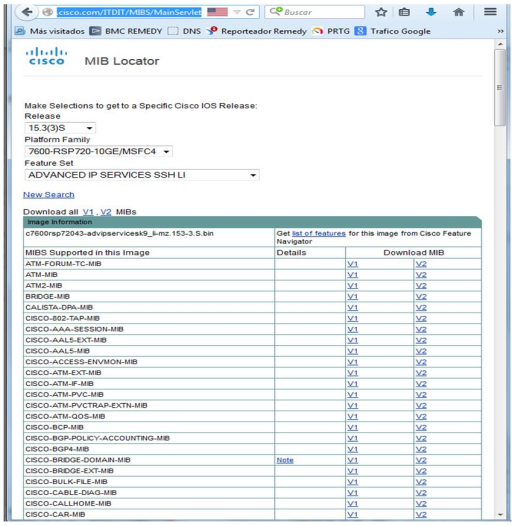


Figura 2.3.1 Búsqueda MIB CISCO

Seleccionando el equipo y pulsando un clic en la MIB ya sea V1 o V2 se obtendrá la información de la misma.

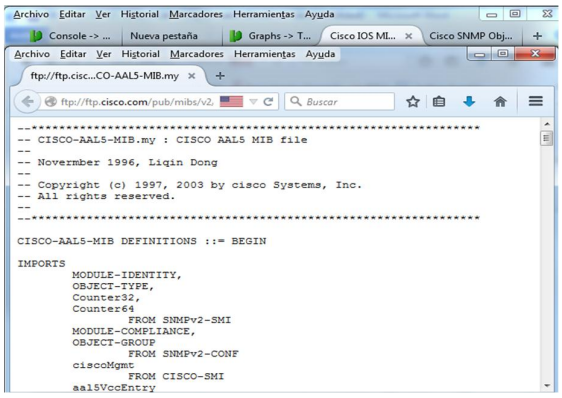


Figura 2.3.2 Información MIB CISCO

También CISCO proporciona otra página para búsqueda de las MIB en la siguiente url: http://tools.cisco.com/Support/SNMP/do/SearchOID.do, ingresar el nombre del objeto que deseo consultar, selecciono buscar y

desplegará la información relacionada.

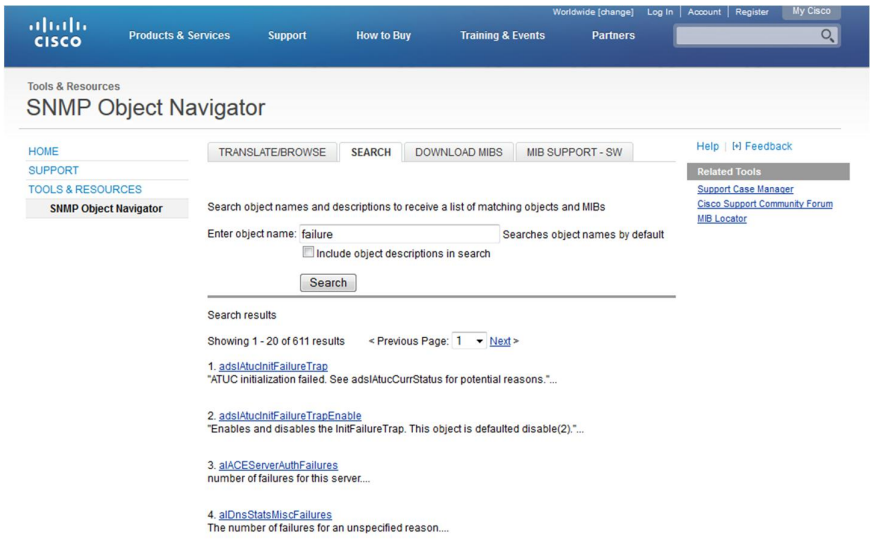


Figura 2.3.3 Información objetos SNMP CISCO

Seleccionamos el MIB y se obtiene la información del OID del objeto SNMP CISCO consultado.

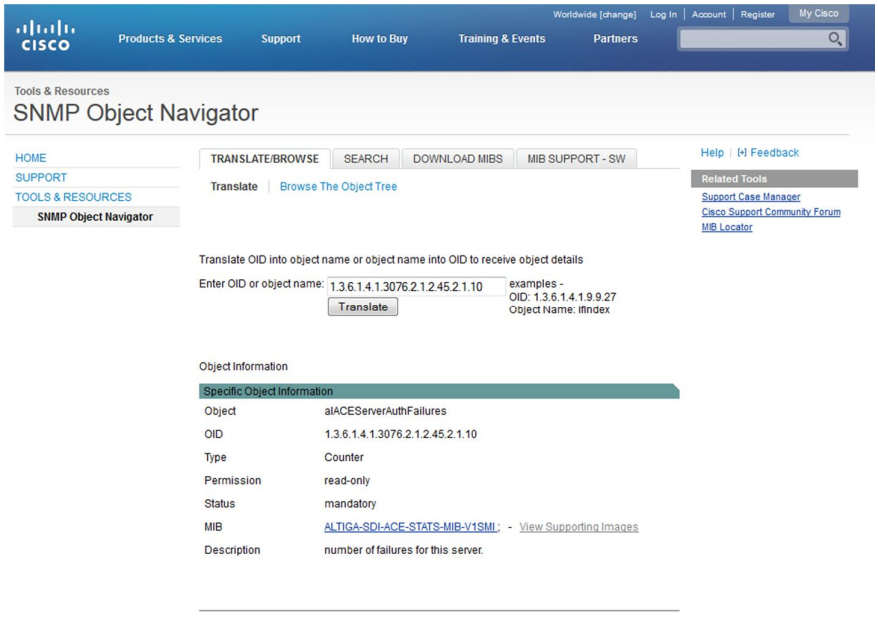


Figura 2.3.4 Información OIDs del objeto SNMP CISCO

b. Podemos consultar en cada equipo accediendo mediante SSH:

En la Figura 2.3.5 se puede observar que arroja información de las ODIs que tiene este equipo.

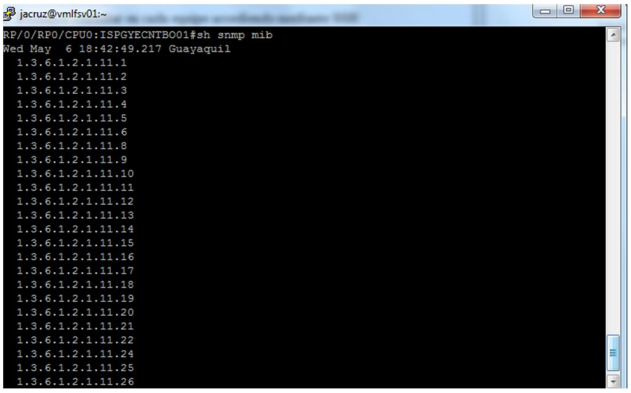


Figura 2.3.5 Información OIDs de un equipo

c. Podemos consultar desde el Data Querie de CACTI :

Para aplicar esta función es necesario tomar las siguientes consideraciones:

- Añadir el equipo en CACTI
- En CACTI por defecto existe una plantilla denominada Cisco Router, la cual recogerá los datos del equipo.
- Se coloca la IP del equipo.
- En CACTI se escogerá SNMP, se configurará la versión, password de los equipos y la encriptación.
- Para que SNMP establezca la conexión el equipo router debe permitir el acceso de la IP que corresponde a CACTI.

Luego de haber realizado las consideraciones indicadas anteriormente, para ingresar a la función Data Querie, debemos ir a dispositivos, seleccionar el equipo, al final de la pantalla seleccionamos SNMP - Interface Statistics que por defecto carga CACTI y aplicamos un clic en consulta detallada:

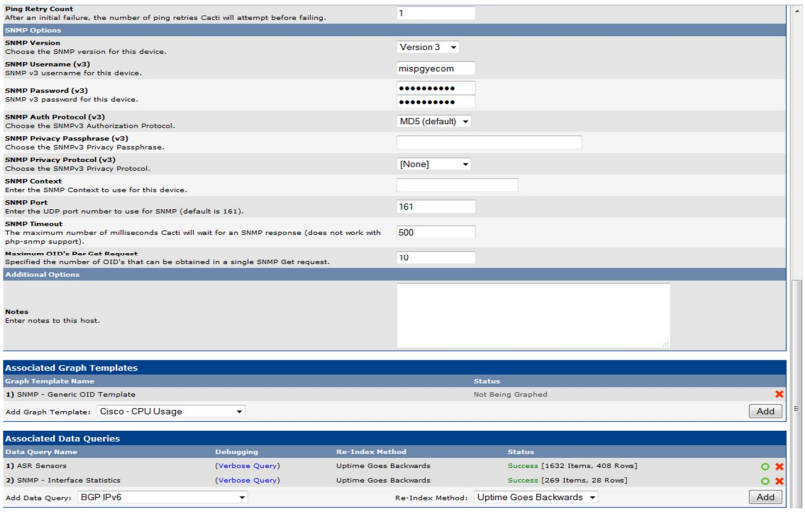


Figura 2.3.6 Objeto SNMP - Interface Statistics CACTI

Para mostrar el resultado de la consulta SNMP – Interface Statistics se usará el equipo de Borde de Guayaquil, dado que los resultados de la consulta son extensos se ha tomado una parte de los resultados obtenidos los cuales se muestran en la Figura 2.3.7.

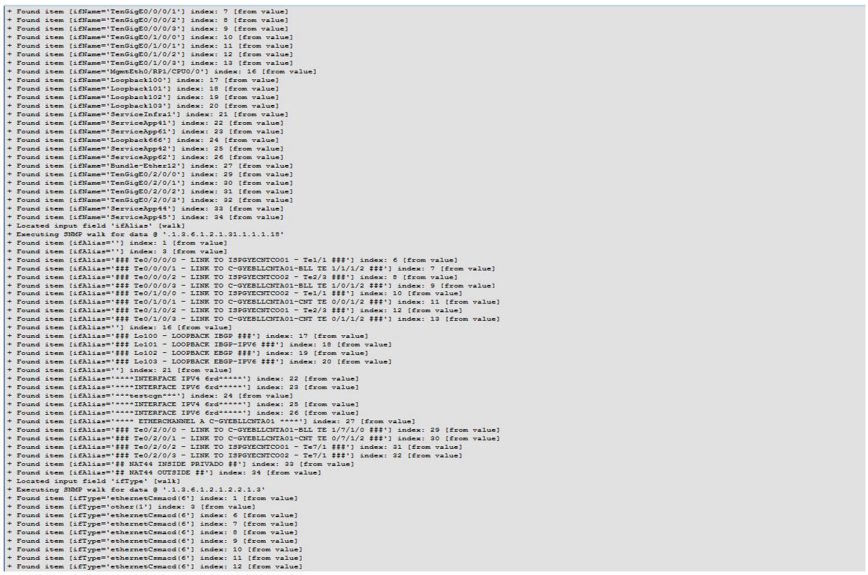


Figura 2.3.7 Información SNMP en CACTI equipo BORDE GYE

En la Figura 2.3.7.1 se muestra otra parte del resultado de la consulta SNMP – Interface Statistics en el cual indica las OIDs como los nombres de los objetos.

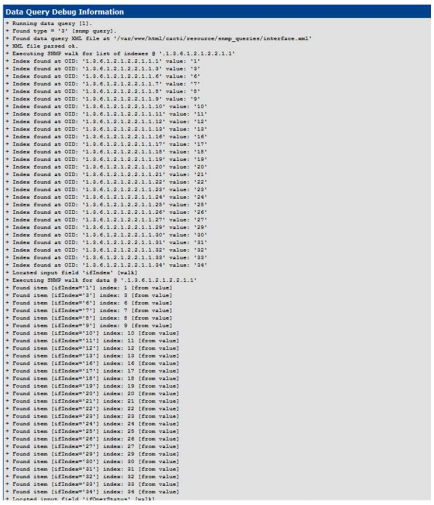


Figura 2.3.7.1 Información OIDs y Object Name en CACTI

A continuación se detalla la información del Objeto obtenido al realizar la consulta SNMP al equipo Borde de Guayaquil.

ifOperStatus	estado operacional actual de la interfaz (up=1 / down=2 / testing=3).
ifDescr	Información de la interfaz
ifIndex	valor único para cada interfaz, su valor se encuentra en el rango de 1 al número de interfaces censadas, en este caso son 34.
ifName	Nombre textual de la interfaz (TenGigE0/0/0/0)
ifAlias	Descripción configurada en la interfaz (Borde)
ifType	Tipo de interfaz, en este caso ethernetCsmacd:6
ifSpeed	Valor aproximado del ancho de banda de la interfaz para este caso indica 4294967295, expresado en bits por segundo.

ifPhysAddress	Dirección física de la interfaz o Mac-address
ifInOctets	Número de octetos (bytes) entrantes en la interfaz
ifOutOctets	Número de octetos (bytes) salientes en la interfaz
ifInDiscards	Número de paquetes entrantes descartados
ifOutDiscards	Número de paquetes salientes descartados
ifInNUcastPkts	Número de paquetes no unicast entrantes
ifOutNUcastPkts	Número de paquetes no unicast salientes
ifInUcastPkts	Número de paquetes unicast entrantes
ifOutUcastPkts	Número de paquetes unicast salientes
ifInErrors	Número de errores entrantes
ifOutErrors	Número de errores salientes
locIfInCRC	Número de CRCs en la interfaz
fIP	Dirección IP de la interfaz

Como se puede observar en el detalle de los objetos entregados mediante SNMP, entre los objetos que pueden ser considerados como indicadores de falla estarían: estado físico de la interfaz (ifOperStatus), paquetes descartados (ifInDiscards, ifOutDiscards), errores (ifInErrors, ifOutErrors), CRC (locIfInCRC), sin embargo se considera necesario incluir más sensores SNMP para evaluar el resultado de cada uno de ellos y considerar que indicadores serán los finales.

Debido a que CACTI es una herramienta de software libre permite la creación de scritps para realizar consultas SNMP específicas de un fabricante, en este caso

CISCO facilita también con la información de los Threshold (umbrales), por lo que el momento de graficar esta información como ya se tiene el umbral definido por CISCO pues muestra las alarmas cuando sobrepasa.

2.3.1 Indicadores de Falla

Como se había indicado en el Modelo de Gestión de Internet de este trabajo, éste usa SNMP para la gestión, la información de MIBs, OIDs, Objetos que se obtiene mediante SNMP es muy extensa, por esa razón es necesario filtrar los indicadores que entreguen información sobre fallas y de estos tomar los que se consideren importantes.

Debido a que SNMP obtiene información de los equipos mediante las MIBs es necesario retomar el concepto de una MIB la cual es una base de datos que recopila OIDs mediante objetos o grupos de objetos relacionados.

MIB trabaja con 11 grupos de Objetos, cada objeto en MIB tiene un identificador de Objeto (OID) por ejemplo dentro del grupo de objetos MIB se encuentra interfaces las cuales manejan una estructura tipo árbol entonces se interpreta de la siguiente manera: ID=1.3.6.1.2.1.2.2.1.8 y su objeto es ifOperStatus, eta información fue detallada y ejemplificada en el ITEM 2.1.2 del presente trabajo.

Con los conceptos claros para obtener información de los OIDs y objetos disponibles por cada equipo se realiza lo siguiente:

- ✓ Se usa Data Querie en CACTI para mediante conexión SNMP nos entregue las OIDs, los objetos disponibles por equipo.
- ✓ Escojo los objetos que entregan información relacionada a fallas para la Gestión de Fallas.
- ✓ Filtro los principales indicadores por cada equipo.

La ventaja de usar CACTI es que podemos, monitorear, graficar los OIDs de los Objetos disponibles en cada equipo y tener resultados, esto depende de la información que dispone cada equipo.

A continuación se presenta la Figura2.3.1.1 que muestra las opciones de SNMP que ofrece CACTI:

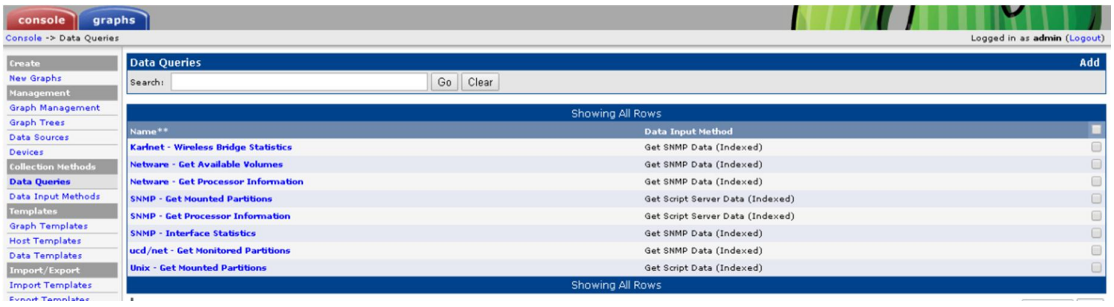


Figura 2.3.1.1 Información SNMP en CACTI

De acuerdo a la Figura 2.3.1.1 en CACTI se tiene el siguiente sensor SNMP que se relaciona con Gestión de Fallas:

SNMP – Interface Satistics es un sensor que viene por defecto cargado en CACTI.

- SNMP – Interface Statistics: se utiliza para consultar tráfico, errores y estado de cada interfaz de los equipos. Existen varias consultas asociadas a éste.

    - In/Out Bits (64-bit Counters): consulta el tráfico en la interfaz.
    - In/Out/Errors/Discarded Packets: consulta los errores en una interfaz
    - Status: consulta el estado de una interfaz.

CACTI brinda consultas de los monitoreos en línea, diario, semanal, mensual y anual. También permite monitoreo y grafico de los paquetes descartados in/ out, errores in/ ut, crsc, estatus físico de la interfaz y tráfico.

A continuación se detallan los sensores SNMP que debido a experiencias en el área, en otra áreas internas de CNT y reportes de fallas recurrentes se vio necesario configurar mediante script y cargarlos en CACTI de acuerdo a la información que entrega cada equipo de comunicaciones de ISP, cabe recalcar que la información de OIDs para realizar estas consultas en CACTI fue obtenida de la información que

proporciona CISCO como se había detallado en el ITEM 2.3 del presente trabajo.

- SNMP - Cisco BGP Neighbor State & Uptime: consulta el estado y uptime de la sesión BGP con el vecino. Muestra el monitoreo realizado a la sesión BGP del equipo, el proceso BGP consiste de 6, la interacción con otros procesos BGP se lleva a cabo intercambiando mensajes. Los mensajes intercambiados en una sesión BGP sirven para informar sobre el conocimiento de nuevas rutas activas, suprimir rutas que ya no estén activas, mostrar la posibilidad actual de la conexión.

Los posibles estados son: libre, en conexión, activo, envío de mensaje de identificación (opensent), respuesta al mensaje de indentificación (openconfirm), se aceptan las identificaciones (established), es decir la sesión está completa y activa.

- SNMP - Cisco Memory Usage: consulta el uso de la memoria interna del equipo.
- SNMP - Cisco Power: consulta el consumo de corriente del equipo.
- SNMP - Cisco Sensors - Optical Power: consulta la potencia óptica de la recepción y transmisión de la interfaces en dbm.
- Cisco Sensors – Temperature: consulta la temperatura por dispositivo del equipo.
- SNMP - Cisco System Uptime: consulta el tiempo que ha transcurrido desde el último reinicio del equipo.

CACTI también permite monitorear conectividad de equipos utilizando PING, el monitoreo indica información diaria de porcentajes y promedios de los paquetes perdidos, latencia.

2.4 DEFINICIÓN DE LOS INDICADORES DE FALLAS

CNT EP trabaja bajo la norma ISO 9000 la cual está alineada en la calidad de redes de Telecomunicaciones, una de las ventajas que ofrece esta norma es la de reducir las incidencias de prestación de servicios por lo que define la confiabilidad como la probabilidad de que un dispositivo o sistema funcione adecuadamente, para un intervalo de tiempo y bajo condiciones de operación determinados. Esto se lo puede realizar con los mantenimientos preventivos, calidad de los equipos, condiciones de excepción contraladas etc.

Esta norma considera los siguientes términos y definiciones: [7][21]

- Indisponibilidad: lo define como un evento en que un componente o sistema quede fuera de servicio por una falla.
- Confiabilidad: lo define como la relación del intervalo libre de falla.
- Disponibilidad: lo define como la relación del tiempo de uso.

[21]Referencia bibliográfica [7] (ISO, 2008)

Es importante mencionar la ISO 9000 y sus conceptos ya que de ésta parte la definición de los indicadores de falla obtenidos para el presente trabajo.

Haciendo relación los conceptos del ISO 9000 los indicadores de falla deben estar enfocados en mantener la disponibilidad y confiabilidad en la prestación de servicios, evitando o mitigando la indisponibilidad de los mismos. Entonces estamos hablando de una disponibilidad de red que no genere fallas en los servicios.

El ISP es un proveedor de servicios de Internet, pero Internet mediante el protocolo IP está diseñado para trabajar como un mecanismo de mejor esfuerzo (Best-effort), no garantiza que los datos lleguen a su destino, ni ofrece a un usuario calidad de servicios, para contrarrestar este mecanismo de internet, se debe aplicar calidad de servicio en las configuraciones en las comunicaciones, en los equipos de comunicaciones de ISP no se encuentra configurado, esto lo hacen a nivel del acceso y salidas internacionales que es administrada internamente por otra área de CNT, sin embargo esto no genera una falla del servicio ya que la navegación que es la esencia habrá, aplicar calidad de servicio sería telefonía, streaming de video u otras aplicaciones que requieran calidad de servicio.

Para que la prestación del servicio no se vea afectada se basa en la disponibilidad de los equipos por los cuales se configura el mismo, y en la existencia de equipos de

reserva. Es decir el mantenimiento está directamente relacionado con la disponibilidad de los equipos, manteniendo la confiabilidad de cada uno de ellos y mejorando su mantenibilidad. Para esto se necesita tener indicadores de falla de los equipos en función de su impacto global con el fin de facilitar la toma de decisiones.

Los análisis de fallas de los equipos de comunicaciones del ISP se realizan de manera reactiva, es decir solo en caso de que un evento ocurre y afecte la normal operación, al no tener un modelo de gestión de fallas que identifique claramente las actividades a realizar en base a cada indicador, muchas veces ocasiona que se hagan actividades que no están enfocadas a cumplir este objetivo.

Basada en las fallas registradas en bitácora, que se han presentado entre los años 2012/2014 en los equipos de comunicaciones, y que en su mayoría han generado indisponibilidad a la prestación del servicio, se obtuvo los indicadores de falla que se muestran en la Tabla2.4.1. La elección de los mismos estuvo enfocada en el impacto que genera en la prestación del servicio al afectarse cada uno de ellos y también en el grado de confiabilidad que se puede tener en los equipos.

Con lo expuesto anteriormente el presente trabajo se enfoca en definir los indicadores que pueden generar posibles causas de una falla y la elaboración de procedimientos que prevean las mismas o ayude a controlarlas.

En el ITEM 2.3 del presente trabajo se indica cómo obtener a través de SNMP mediante el gestor CACTI la información de objetos relacionados con los indicadores de falla, la información es obtenida de los equipos de comunicaciones de ISP y con ésta se ha elaborado la Tabla2.4.1 en la cual podemos observar los principales indicadores de falla que podemos obtener de los equipos de comunicaciones de ISP.

INDICADOR	CONSULTA SNMP	UNIDAD	PERIODO DE LA CONSUTA SNMP	OBTENCIÓN (DATA QUERIES) EN CACTI	DONDE SE MIDE
USO DE CPU	Porcentaje de uso del CPU	%	Cada 5 minutos	Cisco - CPU Usage	Procesador del equipo
SESION BGP	Estado de la sesión BGP con el Vecino	días	Cada 5 minutos	SNMP - Cisco BGP Neighbor Statistics	Vecino BGP, En cada Interfaz
MEMORIA USADA	Bytes de Memoria Usada	Bytes	Cada 5 minutos	SNMP - Cisco Memory Usage	Memoria del equipo
POWER	Corriente Total Disponible	centiAmpsAtXXVolts	Cada 5 minutos	SNMP - Cisco Power	Fuente de poder del equipo
POWER	Potencia óptica de la recepción	dbm	Cada 5 minutos	SNMP - Cisco Optical Power	En cada interfaz
DISPONIBILIDAD DEL SISTEMA	Tiempo de Uptime del Equipo	Segundos	Cada 5 minutos	SNMP - Cisco System Uptime	Procesador del equipo
TEMPERATURA	Valor de temperatura del dispositivo	Grados Celsius	Cada 5 minutos	SNMP - Cisco Temperature	Estadísticas recolectadas por cada dispositivo con sensor de temperatura en el equipo
TRAFICO	ancho de banda aproximado de la interfaz	bits/sec	Cada 5 minutos	Interface - Traffic (bits/sec, Total Bandwidth)	En cada interfaz

ESTADO FISICO DE LA INTERFAZ	estado operacional actual de la interfaz	up=1 / down=2	Cada 5 minutos	SNMP - Interface Statictis	En cada interfaz
PAQUETES DESCARTADOS ENTRANTES	Número de errores entrantes	errors/sec	Cada 5 minutos	ifInErrors	En cada interfaz
PAQUETES DESCARTADOS SALIENTES	Número de errores salientes	errors/sec	Cada 5 minutos	ifOutErrors	En cada interfaz
ERRORES EN LA INTERFAZ	Número de CRCs en la interfaz	errors/sec	Cada 5 minutos	locIfInCRC	En cada interfaz
LATENCIA	Tiempo de retardo para llegar los paquetes	mseg	Cada 5 minutos	Advanced Ping (ICMP)	En cada interfaz

Tabla2.4. Principales indicadores de falla para equipos de comunicaciones de ISP

Una vez obtenido los indicadores de falla, es necesario indicar los umbrales con los cuales se configura estos indicadores en la herramienta de monitoreo CACTI. Los umbrales detallados de acuerdo a cada indicador entonces son:

- USO DE CPU: en este indicador se definió el valor de umbral mayor o igual al 85% debido a que por recomendaciones técnicas del proveedor estos equipos deben trabajar con un valor menor al 85% de su ocupación de memoria.

- SESION BGP: en este indicador se definió el valor de umbral diferente de 6 debido a que para que se establezca la sesión BGP debe cumplir 6 pasos: Idle=1, connect=2, active=3, opensent=4, openconfirm=5, established=6.

- MEMORIA USADA: en este indicador se definió el valor de umbral mayor o igual al 85% debido a que por recomendaciones técnicas del proveedor estos equipos deben trabajar con un valor menor al 85% de su ocupación de memoria.

- POWER: Los valores de corriente son para cada equipo, por esa razón el valor está definido por el proveedor en los OIDs del equipo.

- POWER INTERFAZ: en este indicador se definió el valor de umbral recomendado por el proveedor de acuerdos a sus OIDs.

- DISPONIBILIDAD DEL SISTEMA: Este valor está definido de acuerdo a la experiencia en Operación y Mantenimiento de acuerdo al siguiente criterio: sin un equipo tiene un up time de una hora y, se descarta apagado por mantenimiento o evento de energía en un nodo, se debe revisar la causa por la que se está reiniciando ya que puede generar afectación a la data que contiene.

- TEMPERATURA: en este indicador se definió el valor de umbral recomendado por el proveedor de acuerdos a sus OIDs.

- TRAFICO: Los valores están definido de acuerdo a la experiencia en Operación y Mantenimiento de acuerdo al siguiente criterio: si una interfaz pierde tráfico sobre el 30% del total de la capacidad ese tráfico, indica que algo pasa, por lo que se debe revisar la causa. Si la interfaz sobrepasa el 85% de la ocupación se debe revisar si el comportamiento es normal por consumo o si existe algún evento que ocasionó ese incremento.

- ESTADO FISICO DE LA INTERFAZ: debido a que la interfaz física se encuentra únicamente en dos estados 1= UP y 2=DOWM, en este indicador se definió el valor de umbral = 2.

- PAQUETES DESCARTADOS ENTRANTES: en este indicador se definió el valor de umbral 1 debido a que si hay un paquete descartado entrante ya se debe revisar.

- PAQUETES DESCARTADOS SALIENTES: en este indicador se definió el valor de umbral 1 debido a que si hay un paquete descartado saliente ya se debe revisar.

- ERRORES EN LA INTERFAZ: este valor está definido de acuerdo a los OIDs del proveedor en cada equipo.

- LATENCIA: La latencia se mide entre dos puntos, corresponde al tiempo de respuesta para la entrega de los paquetes por lo que es una medida que tiene variaciones, entonces en este proyecto el valor máximo de latencia estará dado de acuerdo al comportamiento de la misma para un equipo durante el tiempo de un mes.

A continuación se visualiza en la Tabla2.5 los indicadores de falla con sus respectivos umbrales:

INDICADOR	CONSULTA SNMP	UNIDAD	PERIODO DE LA CONSUTA SNMP	OBTENCIÓN (DATA QUERIES) EN CACTI	DONDE SE MIDE	UMBRALES
USO DE CPU	Porcentaje de uso del CPU	%	Cada 5 minutos	Cisco - CPU Usage	Procesador del equipo	>=85%
SESION BGP	Estado de la sesión BGP con el Vecino	días	Cada 5 minutos	SNMP - Cisco BGP Neighbor Statistics	Vecino BGP, En cada Interfaz	≠ 6
MEMORIA USADA	Bytes de Memoria Usada	Bytes	Cada 5 minutos	SNMP - Cisco Memory Usage	Memoria del equipo	>=85%
POWER	Corriente Total Disponible	centiAmpsAtXXVolts	Cada 5 minutos	SNMP - Cisco Power	Fuente de poder del equipo	> carga del equipo
POWER INTERFAZ	Potencia óptica de la recepción y transmisión	dbm	Cada 5 minutos	SNMP - Cisco Optical Power	En cada interfaz	> = -X dbm de la OID provista por el proveedor
DISPONIBILIDAD DEL SISTEMA	Tiempo de Uptime del Equipo	Segundos	Cada 5 minutos	SNMP - Cisco System Uptime	Procesador del equipo	<= 1 hora

TEMPERATURA	Valor de temperatura del dispositivo	Grados Celsius	Cada 5 minutos	SNMP - Cisco Temperature	Estadísticas recolectadas por cada dispositivo con sensor de temperatura en el equipo	= umbral provista por el proveedor
TRAFICO	ancho de banda aproximado de la interfaz	bits/sec	Cada 5 minutos	Interface - Traffic (bits/sec, Total Bandwidth)	En cada interfaz	<= 30% de la capacidad total de la interfaz ó > 85%
ESTADO FISICO DE LA INTERFAZ	estado operacional actual de la interfaz	up=1 / down=2	Cada 5 minutos	SNMP - Interface Statictis	En cada interfaz	= 2
PAQUETES DESCARTADOS ENTRANTES	Número de errores entrantes	errors/sec	Cada 5 minutos	ifInErrors	En cada interfaz	> 0
PAQUETES DESCARTADOS SALIENTES	Número de errores salientes	errors/sec	Cada 5 minutos	ifOutErrors	En cada interfaz	> 0
ERRORES EN LA INTERFAZ	Número de CRCs en la interfaz	errors/sec	Cada 5 minutos	locIfInCRC	En cada interfaz	> 0
LATENCIA	Tiempo de retardo para llegar los paquetes	mseg	Cada 5 minutos	Advanced Ping (ICMP)	En cada interfaz	Valor definido por el comportamiento durante un mes

Tabla2.5. Principales indicadores de falla con umbrales

2.5 MONITOREO DE LOS INDICADORES

En base a lo expuesto en el ITEM2.3 el cual trata sobre la revisión y obtención de los principales indicadores por Equipo, a continuación se muestra el monitoreo obtenido de los indicadores:

La Figura 2.5.0 muestra el monitoreo realizado sobre el uso del CPU del equipo CORE del ISP, durante el día permanece en un porcentaje menor al 5%, sin embargo el día anterior hubo un pico al 15%.

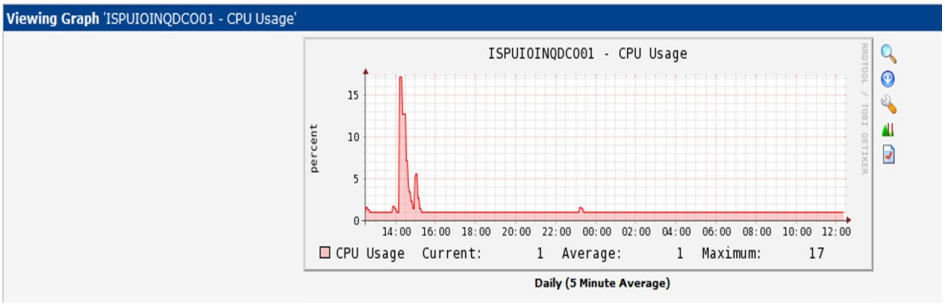


Figura 2.5.0 Cisco ï CPU Usage

La Figura 2.5.1 muestra el monitoreo realizado a la sesión BGP del equipo de borde de Guayaquil, como se puede observar en la gráfica el proceso BGP consiste de 6 estados, los cuales se describen a continuación:

Idle: Libre

Connect: en conexión

Active: activo,

OpenSent: envío de mensaje de identificación

OpenConfirm: respuesta al mensaje de identificación

Established: se aceptan las identificaciones, es decir la sesión está completa y activa.

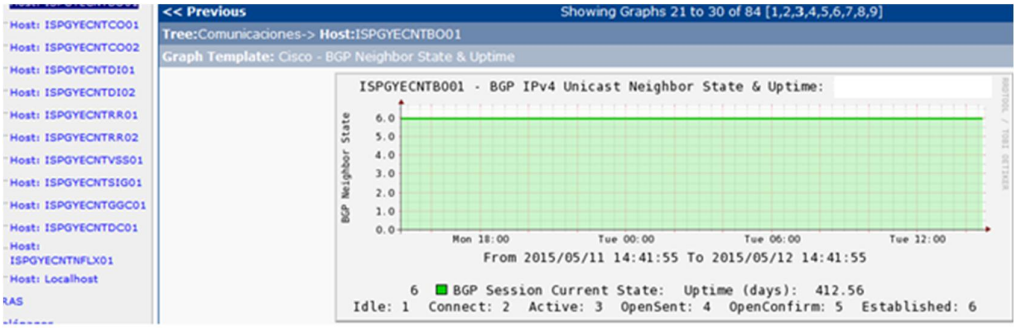


Figura 2.5.1 Cisco ï BGP Neighbor State & Uptime

En la Figura 2.5.2 se puede observar el monitoreo o consulta del uso de la memoria interna del equipo y también de la memoria libre del equipo, para este ejemplo del equipo de Borde de Guayaquil se muestra que del total de memoria que dispone el equipo que es 3.73G se encuentra usada 1.55G.

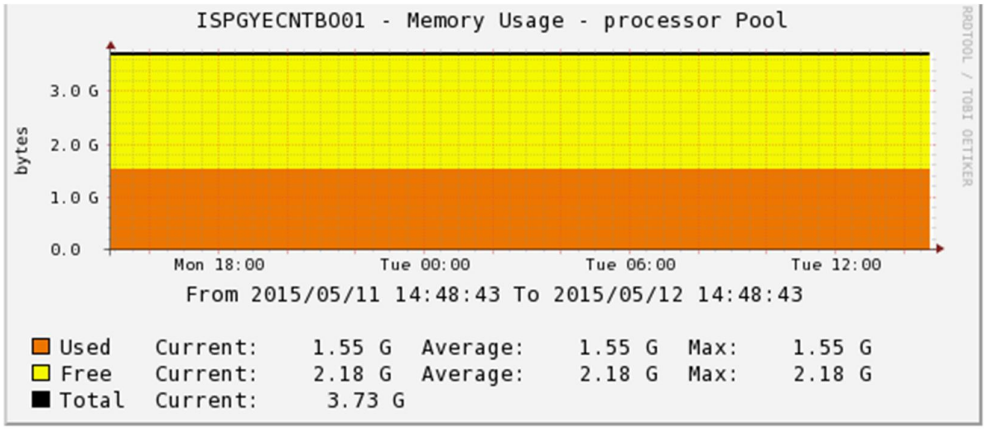


Figura 2.5.2 SNMP - Cisco Memory Usage.

En la Figura 2.5.3 se puede observar el monitoreo o consulta del consumo de corriente del equipo Core de Guayaquil, el valor 85,58 amperios corresponde al

consumo y el valor 137,42 corresponde a la carga que soporta el equipo, también indica que está conectado en energía DC (42v).

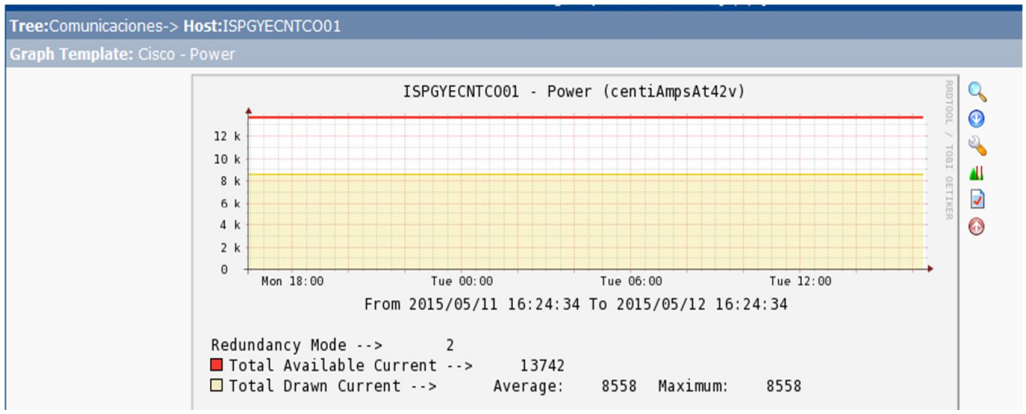


Figura 2.5.3 SNMP - Power

En la Figura 2.5.4 se puede observar el monitoreo o consulta de la potencia óptica de la recepción de la interfaz Te1/1 en dbm la cual indica que la potencia óptica es de -9,50 dbm, para este caso el umbral es -15 dbm de la OID provista por el proveedor. También existe una alerta alta cuando el umbral llega a 1.

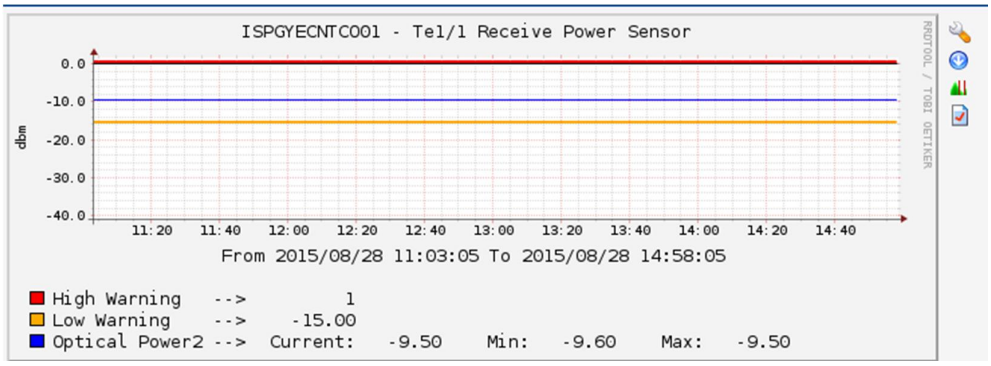


Figura 2.5.4 SNMP - Cisco Optical Power

En la Figura 2.5.5 se puede observar el monitoreo o consulta del tiempo que ha transcurrido desde el último reinicio del equipo, entonces indica que este equipo Borde de Guayaquil se encuentra UP hace 51 días.

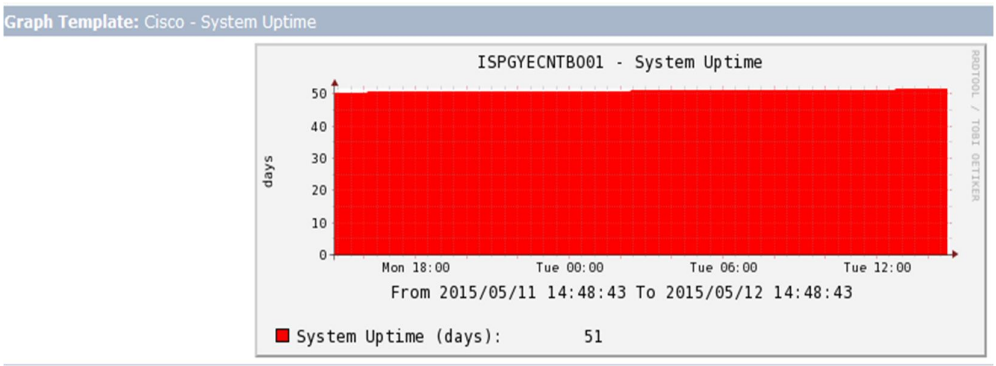


Figura 2.5.5 SNMP - Cisco System Uptime

En la Figura 2.5.6 se puede observar el monitoreo o consulta de la temperatura censada a la tarjeta procesadora del equipo de Distribución de Quito, para este ejemplo indica el valor del consumo en grados Celsius de la entrada corresponde a 39 y de la salida de 43 Celsius. También se encuentra configurado un umbral de acuerdo a la OID dada por el proveedor con un valor de 65 Celsius tanto para la entrada como para la salida.

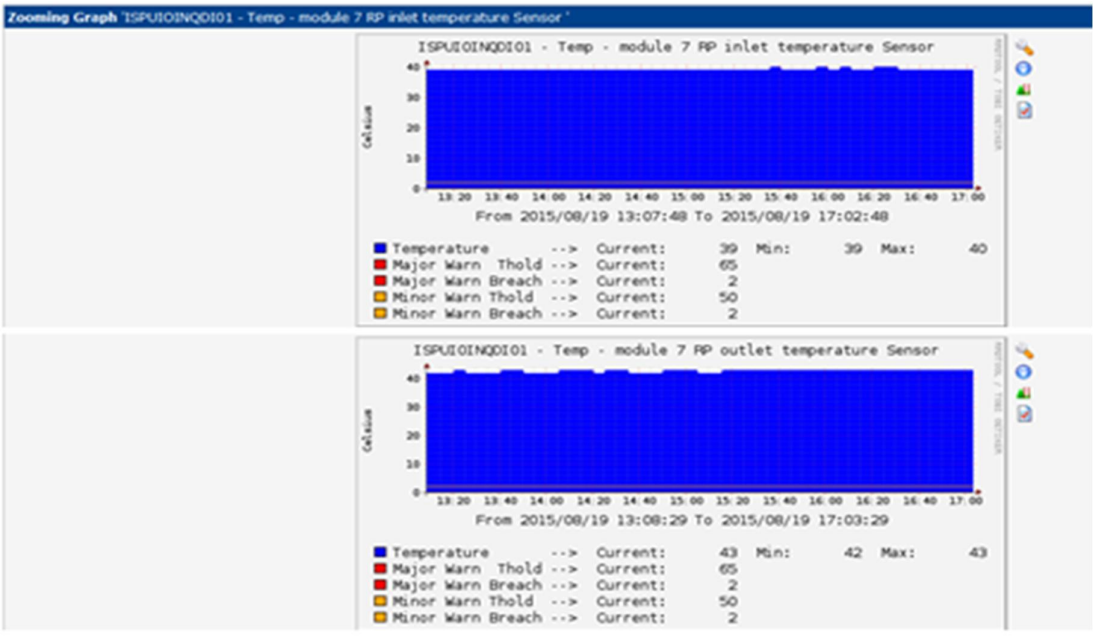


Figura 2.5.6 Cisco Sensors ï Temperature

En la Figura 2.5.7 se puede observar el monitoreo o consulta del Tráfico de la Interfaz Te0/0/0/0 del equipo de comunicaciones BORDE hacia la interfaz Te1/1 del equipo de comunicaciones CORE, estas interfaces físicamente soportan 10G y el consumo de acuerdo a la Gráfica indica sobre los 8G.

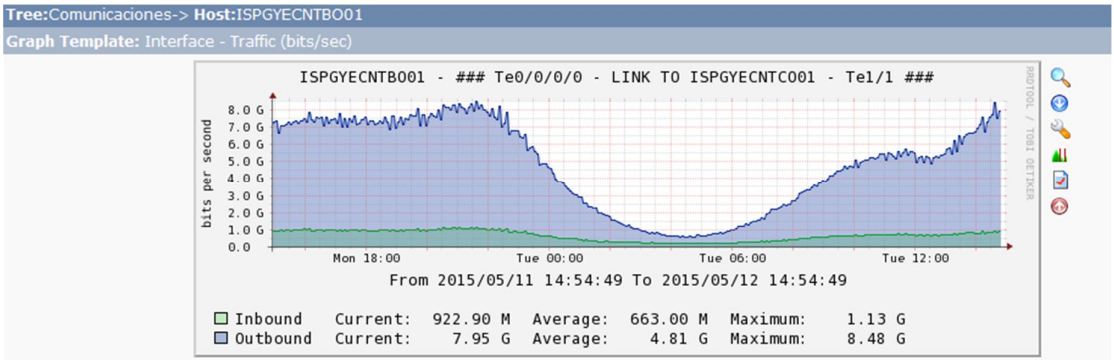


Figura 2.5.7 Tráfico de la Interfaz ISPGYECNTBO01 hacia ISPGYECNTCO01

En la Figura 2.5.8 se puede observar el monitoreo o consulta del estado físico de la interfaz de acuerdo a sus estados: 1 es Up y 2 es Down, para este ejemplo la Interfaz Te0/0/0/0 del equipo de comunicaciones BORDE hacia la interfaz Te1/1 del equipo de comunicaciones CORE se encuentra UP.

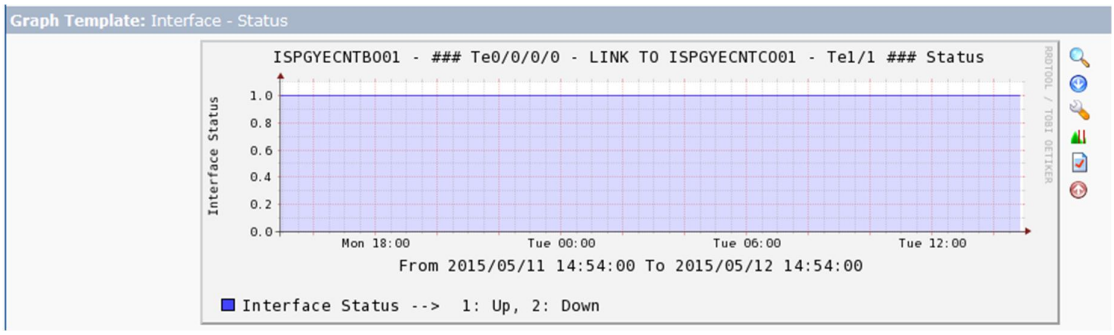


Figura 2.5.8 Estado Físico de la Interfaz

En la Figura 2.5.9 se puede observar el monitoreo o consulta de paquetes descartados In/Out, errores In/Out y CRCs para este ejemplo de la Interfaz Te0/0/0/0 del equipo de comunicaciones BORDE hacia la interfaz Te1/1 del equipo de comunicaciones CORE, como se puede observar tiene un valor 0.

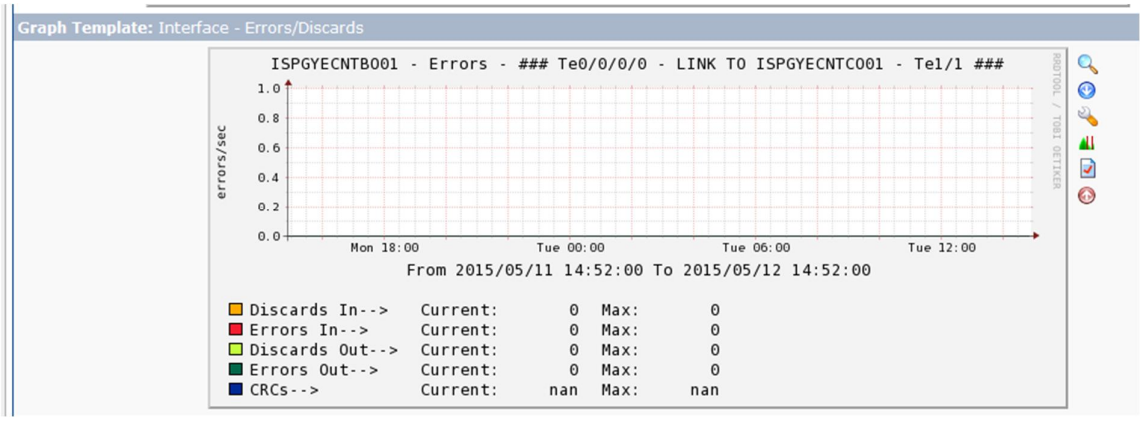


Figura 2.5.9 Paquetes descartados, errores, CRCs.

En la Figura 2.5.10 se puede observar el monitoreo o consulta de ping hacia el equipo de comunicaciones BORDE de Guayaquil, para este ejemplo muestra como resultado 0 paquetes perdidos, respuesta promedio de ping o latencia de 9.89 ms. De igual manera se puede observar el monitoreo o consulta de ping hacia el equipo de comunicaciones BORDE de Quito, para este ejemplo muestra como resultado 0 paquetes perdidos, respuesta promedio de ping o latencia de 4.18 ms. Hay que tener en cuenta que el cálculo de la LATENCIA que se está realizando es desde el servidor CACTI hacia el equipo de comunicaciones.

La lógica de CACTI por default realiza 20 pines por cada 5 minutos, entonces hace 4 pines por cada minuto y como cada minuto tiene 60 segundos entonces la consulta de ping es cada 15 segundos.

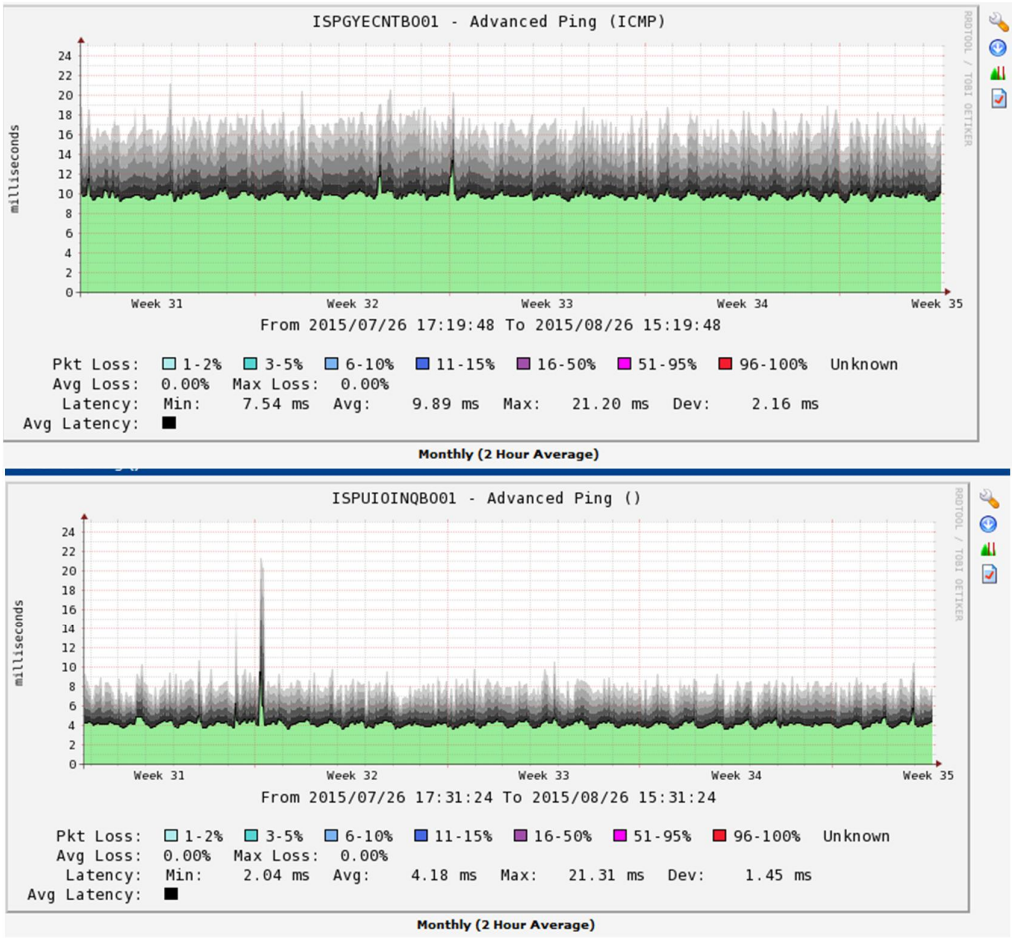


Figura 2.5.10 Resultado de consultas PING en CACTI

3. CAPITULO III – PROCESOS DE GESTION DE FALLAS

3.1 METODOLOGIA DE ATENCIÓN DE FALLAS

3.1.1 Descripción de los procesos inmersos dentro de las principales funciones de gestión de fallas.

Como se expuso en el capítulo II, Gestión de Fallas son un conjunto de actividades que permiten la detección de la ocurrencia de falla, el aislamiento de la causa de la falla y la corrección de la misma que pudiesen ocurrir en las redes o sistemas de comunicaciones permitiendo mantener activamente el nivel de servicio de la red.

Entre las funciones principales de gestión de fallas se detalla:

1. Supervisión del estado de la red: mediante herramienta de monitoreo.
2. Detección de problemas: mantenimiento preventivo.
3. Respaldo y configuración: generación de respaldos puede ser automático o manual.
4. Diagnóstico y Reparación: mantenimiento correctivo.

Para la metodología de atención de fallas se describirá los procesos que se encuentran inmersos dentro de cada una de las funciones de gestión de fallas indicadas.

Supervisión del estado de la red

Para la supervisión del estado de la red de equipos de comunicaciones de ISP, de acuerdo a lo expuesto en el capítulo II se utiliza la herramienta de gestión de monitoreo web CACTI, esta es de software libre o código abierto, busca automáticamente todas las interfaces de un dispositivo, se puede visualizar el monitoreo en tiempo real del estado de las interfaces, utilización de ancho de banda de red, el tráfico de red etc, permite una visualización gráfica de la ingeniería de la red de una manera rápida y cómoda, es muy fácil consultar el estado mediante la visión de las gráficas correspondientes a cada nodo y segmento de equipos dentro del mismo.

En la Tabla2.4.1 del capítulo II se describió los principales indicadores de falla que podemos obtener de los equipos de comunicaciones de ISP, los cuales fueron establecidos de acuerdo al enfoque de mantener la disponibilidad y confiabilidad en la prestación de servicios, es decir disponibilidad de red que no genere fallas en los servicios.

Para desarrollar el procedimiento de supervisión del estado de la red, es necesario basarse en los conceptos que trata norma ISO 9000, la cual considera que la disponibilidad incluye impacto en la prestación de los servicios, por esa razón todos los eventos de corte de red, por causas propias y, las intervenciones programadas

que hayan generado boletas de servicios en ARCOTEL, son consideradas como impactos en los servicios.

CNT EP de acuerdo a los procedimientos mantenidos notifica a ARCOTEL un evento masivo que genere falla total o parcial de la red y que afecte la prestación del servicio, el tiempo para enviar la notificación es cuando haya superado las 3 horas de afectación.

El procedimiento de supervisión del estado de la red, se lo desarrolla mediante la herramienta de monitoreo CACTI con el monitoreo de los indicadores de falla de los equipos de comunicaciones del ISP.

Sin embargo para este procedimiento de supervisión del estado de la red sobre los equipos de comunicaciones de ISP, de acuerdo a lo expuesto sobre la visión de la norma ISO 9000 y, delimitando los indicadores de falla obtenidos, es necesario clasificarlos de acuerdo a un nivel de criticidad.

Un nivel de criticidad está asociado a la afectación, total, parcial o no afectación de la prestación del servicio.

Como se puede observar en la Tabla 3.1.1, el Nivel de Criticidad Alta se asocia a una

falla total de la prestación del servicio, el Nivel de Criticidad Media está relacionado con una falla parcial de la prestación del servicio y el Nivel de Criticidad Baja está ligado a una NO falla en la prestación del servicio.

En la Tabla3.1 se detalle el nivel de criticidad con su respectiva descripción:

Nivel de Criticidad	Descripción
Alta	Interrupción total de servicio en un nodo. Todos los servicios soportados por los equipos estén totalmente caídos, esto puede ocurrir por:
	· Falla completa de los equipos.
	· Imposibilidad de acceso a los equipos para la operación y mantenimiento emergente, debido a que no responden.
Media	Interrupción parcial de servicio en un módulo del equipo, esto puede ocurrir por:
	· Perturbaciones que afecten la parcialmente los servicios o daños de una parte de los componentes o subcomponentes de los equipos.
Baja	Eventos o problemas menores sin impacto en el servicio, esto puede ocurrir por:
	· No tener gestión o monitoreo de los equipos.

Tabla3.1.1 Niveles de Criticidad

Para asociar los indicadores de falla a un nivel de criticidad he analizado el impacto de cada falla es decir los indicadores de falla que se encuentren en criticidad alta son aquellos que necesitan intervención inmediata debido a que pueden o ya ocasionaron pérdida total de la prestación del servicio siempre y cuando no haya otro equipo o elemento redundante.

Los indicadores de falla que se delimiten con criticidad media deben ser atendidos también de manera inmediata ya que a pesar de no afectar totalmente la prestación del servicio pueden o ya ocasionaron pérdida parcial de la prestación del servicio siempre y cuando no haya otro equipo o elemento redundante.

Finalmente los indicadores de falla que se asocien a criticidad baja son aquellos indicadores que no generan afectación a la prestación del servicio, es decir pueden ser atendidos en escenarios de pruebas con equipos o elementos redundantes o en ventanas de mantenimiento.

Una vez definidos los niveles de criticidad y el respectivo análisis de los indicadores respecto a cada nivel, ahora asociaré estos niveles a los indicadores de falla definidos para los equipos de comunicaciones de ISP.

Enlistando los indicadores de Falla mostrados en el Tabla2.4 del capítulo II; en la Tabla 3.1.1.1 se detalla la clasificación que se le da a cada uno basado en la descripción de cada nivel de criticidad de la Tabla3.1.

INDICADOR	CRITICIDAD
USO DE CPU	ALTA
SESION BGP	MEDIA
MEMORIA USADA	ALTA
POWER EQUIPO	ALTA

POWER INTERFAZ	MEDIA
DISPONIBILIDAD DEL SISTEMA	BAJA
TEMPERATURA POR CADA DISPOSITIVO	BAJA
TRAFICO	BAJA
ESTADO FISICO DE LA INTERFAZ	ALTA
PAQUETES DESCARTADOS ENTRANTES	MEDIA
PAQUETES DESCARTADOS SALIENTES	MEDIA
ERRORES EN LA INTERFAZ	MEDIA
LATENCIA	BAJA

Tabla3.1.1.1 Niveles de Criticidad por Indicador

Detección de problemas

Para cumplimiento de la operación y mantención del equipamiento de los equipos de comunicaciones de ISP, se considera las actividades de mantenimiento preventivo como el principal actor, ya que tiene como finalidad lograr la máxima vida de un equipo y detectar posibles problemas. Por esa razón el procedimiento para detección de problemas está ligado al mantenimiento preventivo.

El Mantenimiento preventivo trata de anticiparse a la aparición de fallas, consiste en un grupo de actividades planificadas que se ejecutan periódicamente, con el objetivo de garantizar que los equipos cumplan con las funciones requeridas durante su ciclo de vida útil, con este tipo de mantenimiento se pretende disminuir, evitar o mitigar, la reparación mediante una rutina de inspección periódica y

renovación de los elementos deteriorados.

Respaldos de configuración

Otro procedimiento que se debe considerar y desarrollar es la generación de respaldos de configuración de los equipos de comunicaciones de ISP, esta data es importante debido a que por ejemplo el momento de generarse una falla en la cual involucre cambio de un elemento o cambio total del equipo, es necesario mantener la información de configuración actualizada.

El procedimiento de generación de respaldos de configuración se lo puede realizar de forma automática o manual.

Diagnóstico y Reparación

El proceso de atención de fallas por tradición está enfocado desde el punto de vista del mantenimiento correctivo, por esa razón la función de diagnóstico y reparación está atada al mantenimiento correctivo ya que esencialmente se realiza estas actividades cuando se tiene una falla.

Mantenimiento correctivo: también considerado como mantenimiento reactivo, en este tipo de mantenimiento solo se interviene en los equipos cuando la falla se ha producido.

Las causas que pueden originar un paro imprevisto pueden ser debido a desperfectos no detectados durante las inspecciones predictivas, errores operacionales, ausencia de tareas de rutina.

Para el procedimiento de diagnóstico y reparación es necesario trabajar de acuerdo a los niveles de criticidad indicados en la Tabla3.1 Niveles de Criticidad.

3.1.2 Valores para reportar un indicador de falla

Enlistando los indicadores de Falla mostrados en el Tabla2.4 del capítulo II los cuales fueron relacionados con el nivel de criticidad de la Tabla 3.1.1.1 en la Tabla 3.1.2 se detalla los valores que se le da a cada indicador para su respectivo tratamiento.

INDICADOR	CRITICIDAD	VALORES PARA DETERMINAR UNA FALLA
USO DE CPU	ALTA	>= 85%
SESION BGP	MEDIA	≠ 6
MEMORIA USADA	ALTA	>= 85%
POWER EQUIPO	ALTA	> carga del equipo
POWER INTERFAZ	MEDIA	> = -X dbm de la OID provista por el proveedor
DISPONIBILIDAD DEL SISTEMA	BAJA	<= 1 hora
TEMPERATURA POR CADA DISPOSITIVO	BAJA	= umbral provista por el proveedor
TRAFICO	BAJA	<= 30% de la capacidad total de la interfaz
		ó > 85%
ESTADO FISICO DE LA INTERFAZ	ALTA	= 2

PAQUETES DESCARTADOS ENTRANTES	MEDIA	> 0
PAQUETES DESCARTADOS SALIENTES	MEDIA	> 0
ERRORES EN LA INTERFAZ	MEDIA	> 0
LATENCIA	BAJA	< 90 ms

Tabla3.1.2 Valores para reportar un indicador de falla

A continuación se detalla la explicación de cada valor mostrado en la Tabla3.1.2:

- USO DE CPU: Este valor fue definido de acuerdo a las recomendaciones del proveedor de los equipos por buenas prácticas, en las cuales indican que los equipos cuando ya operan al 85% de su capacidad deben ser ampliados.
- SESION BGP: Este valor está dado de acuerdo a los estados que pasa una sesión BGP para establecerse, es decir cuando el valor es 6 la sesión se encuentra UP y un valor diferente a 6 ocasiona flapeo o caída de la misma, está definido por el proveedor en los ODIs del equipo.
- MEMORIA USADA: Estos valores están definidos de acuerdo al siguiente criterio: si la memoria usada del equipo supera el 85% de la ocupación se debe revisar si el comportamiento es normal por consumo o si existe algún evento que ocasionó ese incremento.
- POWER EQUIPO: Este valor está definido por el proveedor en los OIDs del equipo.
- POWER INTERFAZ: Este valor está definido por el proveedor en los OIDs del equipo.

- DISPONIBILIDAD DEL SISTEMA: Este valor está definido de acuerdo a la experiencia en Operación y Mantenimiento de acuerdo al siguiente criterio: sin un equipo tiene un up time de una hora y se descarta, apagado por mantenimiento o evento de energía en un nodo, se debe revisar la causa por la que se está reiniciando ya que puede generar afectación a la data que contiene.
- TEMPERATURA POR CADA DISPOSITIVO: Este valor de umbral está definido por el proveedor en los OIDs del equipo.
- TRAFICO: Este valor está definido de acuerdo a la experiencia en Operación y Mantenimiento de acuerdo al siguiente criterio: si una interfaz pierde tráfico sobre el 30% del total de la capacidad ese tráfico, indica que algo pasa, por lo que se debe revisar la causa. Si la interfaz sobrepasa el 85% de la ocupación se debe revisar si el comportamiento es normal por consumo o si existe algún evento que ocasionó ese incremento.
- ESTADO FISICO DE LA INTERFAZ: Este valor está definido por el proveedor en los OIDs del equipo.
- PAQUETES DESCARTADOS ENTRANTES: Este valor está definido por el proveedor en los OIDs del equipo.
- PAQUETES DESCARTADOS SALIENTES: Este valor está definido por el proveedor en los OIDs en los OIDs del equipo.
- ERRORES EN LA INTERFAZ: Este valor está definido por el proveedor en los

OIDs en los OIDs del equipo.

- LATENCIA: Este valore está definido de acuerdo al muestreo tomado en los equipos de comunicaciones durante el período de 1 mes.

Estos valores serán usados en todos los procesos a desarrollar en Atención de Fallas.

3.2 DESARROLLAR EL PROCESO DE ATENCION DE FALLAS

En base a la estructura, la organización puede estandarizar los procesos, definir el dueño del proceso y para qué áreas aplica, por lo cual es necesario describir la estructura organizacional de la CNT EP la cual está compuesta por:

Gerencia Coordinadora de Operación y Mantenimiento: es la que coordina con las gerencias bajo su nivel para gestionar temas administrativos y son las siguientes: [1]22.

- Gerencia de O&M: dentro de esta gerencia se encuentra la Jefatura de O&M ISP en la cual se encuentra la plataforma del ISP de la CNT EP y es la responsable de Operar, Mantener y Garantizar la disponibilidad de la prestación del servicio de Internet al igual que la plataforma.

[22] Referencia bibliográfica [1] (CNT, 2014)

- Centro de Operación de Red: se encarga del monitoreo de red y análisis de disponibilidad de servicios, tráfico, desempeño de los equipos y plataformas que conforman la Red de CNT EP, en específico la red del ISP. Esta Gerencia está compuesta por las Jefaturas:
    - Desempeño de red, la cual se encarga de coordinar con el área de Ingeniería para implementar mejoras, ampliaciones o compras para solventar los inconvenientes que presentan vulnerabilidades en los equipos o plataformas de comunicaciones de ISP los cuales pueden ocasionar fallas de los mismos.
    - Centro de Operaciones de Red (NOC), la cual se encarga de monitorear la red de equipos o plataformas de comunicaciones de ISP.
- Gerencia de Transmisiones: es la responsable de brindar la interconexión entre las diferentes centrales mediante anillos metropolitanos, a nivel nacional Fibra Óptica, y MPLS.

Gerencia de Ingeniería e Implementación: es la que coordina con las gerencias bajo su nivel para gestionar temas administrativos y son las siguientes:

- Gerencia de Ingeniería: se encarga de diseñar, definir procesos de mejoramiento, optimización o ampliación de Red, y para los casos en los cuales sus diseños requieran adquirir mediante procesos de compra

equipamiento e implementar las mejoras o ampliaciones de red del ISP.

Desde esta lógica de estructura se determinan las responsabilidades de cada área y las medidas de acción que deben ser ejecutadas mediantes procesos a través de un diagrama de flujo.

Para desarrollar los procesos de atención de fallas trabajaré en función de la estructura organizacional de la empresa con las respectivas actividades que debe realizar cada área siendo una de ellas el monitoreo de los indicadores de falla obtenidos.

De acuerdo a la descripción realizada de cada función de gestión de fallas elaboraré los procesos y ataré al proceso de monitoreo de los indicadores de falla.

A continuación detallaré cada función de gestión de falla con su respectivo proceso, la primera función de falla es la indicada en el ITEM 3.2.1 que corresponde a Supervisión del estado de la Red.

3.2.1 Supervisión del estado de la Red

Como lo había expuesto en el ITEM 3.2, estructura de la organización, las actividades de monitoreo de la red son responsabilidad del área Centro de Operaciones de Red (NOC). Entonces la tarea de monitorear los indicadores de Falla

obtenidos en el presente trabajo corresponde a ésta área.

Cuando NOC verifique o reciba una alarma del indicador de falla debe diferenciar de acuerdo a la criticidad del indicador si es posible atender en ésta área la falla, para esto es necesario trabajar en niveles de responsabilidades.

También es importante recalcar que la función principal que debe cumplir la Jefatura de O&M de Core y Plataformas Internet, TV y Datos es la de operar y mantener los equipos de comunicaciones de ISP.

De acuerdo a lo indicado anteriormente explicaré los niveles de atención ante una falla:

- 1er Nivel: En este nivel NOC es responsable de atender la falla de acuerdo a una MATRIZ REVISIÓN y el nivel de criticidad de los indicadores.
- 2do Nivel: Este nivel es de responsabilidad de O&M ISP, aquí se diagnostica y repara los reportes de fallas sea que afecte o no a la prestación del servicio.

Desarrollando el proceso de supervisión del estado de la red quedaría:

Actividades de NOC

- Monitorear Indicadores de Falla de acuerdo a su nivel de criticidad, valor y MATRIZ REVISIÓN.

- Intervenir nivel 1.

Actividades de O&M

- Configuración del monitoreo en CACTI de los equipos de comunicaciones de ISP de acuerdo a los indicadores de falla.

- Intervenir nivel 2.

3.2.2. Detección de problemas

El procedimiento de detección de problemas se desarrolla mediante las rutinas de mantenimiento preventivo. Cada año se debe elaborar un cronograma que planifique la ejecución de mantenimiento preventivo en los equipos de comunicaciones del ISP, este cronograma debe aprobar la Gerencia O&M y verificar el cumplimiento mediante reportes mensuales.

Para los casos en los cuales dentro del mantenimiento preventivo se descubra un requerimiento de mejora o ampliación, el área que debe analizar este requerimiento de acuerdo a la estructura organizacional debe ser Ingeniería, una vez atendido este requerimiento debe generar una orden de trabajo para la ejecución de la ampliación o mejoramiento.

Esta orden de trabajo debe ser coordinada su implementación entre las áreas de desempeño de la red e ingeniería y ejecutada por el área de O&M ISP.

Desarrollando el proceso de detección de problemas quedaría:

Actividades de O&M ISP

- Elaborar Cronograma para planificación de ejecución de mantenimientos preventivos.

- Solicitar aprobación a la Gerencia O&M

- Ejecutar el cronograma de mantenimientos preventivos.

- Elaborar reporte de cumplimiento mensual.

- Enviar reporte mensual de cumplimiento a la Gerencia de O&M.

Actividades de Gerencia O&M

- Aprobar cronograma de mantenimiento preventivo.

- Verificar cumplimiento.

Actividades de Gerencia Ingeniería

- Verificar y analizar requerimiento de mejora o ampliación.

- Generar Orden de Trabajo

Actividades de Desempeño de Red

- Registrar Orden de Trabajo

- Gestionar Cambios

- Incorporar el plan de mantenimiento en el sistema.

En este proceso se debe atender los indicadores de falla orientados a realizar un análisis en ambiente de pruebas, es decir, si se genera una alarma de este indicador no afecta a la prestación del servicio pero previene de que algo puede afectar el mismo, si no se toma acción. Por lo tanto los indicadores que se definieron en base a este pensamiento fueron los de criticidad baja, entonces esos indicadores serán considerados dentro de este proceso.

3.2.3 Respaldos de configuración

Para desarrollar el procedimiento de generación de respaldos de configuración se tiene que configurar que el grabado se lo realice de forma automática cada 12 horas o cada vez que se realiza un cambio en la configuración del equipo de comunicaciones de ISP y se guarde la misma. La configuración de respaldo se debe guardar en un servidor FTP.

Desarrollando el proceso de Respaldos de configuración quedaría:

Actividades de O&M ISP

- Solicitar configuración de los comandos de obtención de respaldos.

- Configurar en los equipos de comunicaciones de ISP la obtención de los respaldos de la configuración y envío hacia un servidor FTP cada 12 horas.

- Configurar en los equipos de comunicaciones de ISP la obtención los respaldos

dela configuración y envío hacia un servidor FTP cada vez que se grabe la configuración.

- Comprobar correcta ejecución.

- Revisar semanalmente que la data del servidor FTP esté actualiza con el último archivo guardado y validar que sea legible.

Este proceso también es importante debido a que se debe contar con la información actualizada de la configuración de los equipos, dentro de la configuración respaldada se encuentra la configuración de comandos que permiten las consultas SNMP hacia los equipos, ésta parte es importante dentro de este proyecto ya que si no se cuenta con los permisos no se podría monitorear los indicadores de Falla definidos para cada equipo.

3.2.4 Diagnóstico y Reparación

El procedimiento de diagnóstico y reparación se lo realiza mediante las rutinas de mantenimiento correctivo. O&M ISP debe realizar las acciones necesarias para diagnosticar y reparar la falla.

Desarrollando el proceso de Diagnóstico y Reparación quedaría:

Actividades de O&M ISP

- Diagnosticar o detectar la Falla.

- Reparar la Falla

- Elaborar informe de solución de la Falla

- Enviar informe de la solución de la Falla a NOC.

En este proceso se debe atender los indicadores de falla que afectan parcial o total la prestación del servicio , es decir, si existe una alarma de este indicador se debe tomar acciones inmediatas debido a que puede o ya ocasionó una falla en la prestación del servicio. Se puede confundir en por qué no prevenir antes de que se dé la falla pero debemos recordar que estos indicadores de falla están caracterizados algunos porque tienen dos estados up o down, otros porque si su procesamiento eleva al máximo no responde el equipo y otros de apagado del equipo, entonces no permiten análisis previo a pesar de que pueden tener umbrales ya que en algunos casos existen eventos que ocurren de manera inesperada. Por lo tanto los indicadores que se definieron en base a este pensamiento fueron los de criticidad alta y media, entonces esos indicadores serán considerados dentro de este proceso.

3.3 DEFINICION Y ELABORACION DE LOS PROCESOS

La CNT EP está considerada como la empresa pública pionera en la provisión del servicio de Internet a nivel Nacional. Las fallas en los equipos de comunicaciones del ISP de la CNT EP, pueden ocasionar una pérdida de la continuidad del suministro de Internet tanto para clientes considerados dentro del segmento masivo como los

clientes del segmento corporativo.

Por este motivo es necesario plantear procedimientos para detectar, corregir circunstancias o eventos de falla que pudiesen ocurrir en los equipos de comunicaciones de ISP, esto en el menor tiempo posible o mantener activamente el nivel de servicio de la red, para lo cual es necesario definir y elaborar procesos.

Para la definición y elaboración de los procesos se clasificó los indicadores de falla de los equipos de comunicaciones de ISP de acuerdo a su nivel de criticidad y éste a su vez se clasificó en base a la afectación en la prestación del servicio.

Como se había explicado en el Capítulo II es importante definir si la falla genera un alto, medio o baja impacto sobre el servicio, esta definición está enfocada hacia el servicio de Internet. CNT EP responde al ente regulador ARCOTEL por la disponibilidad de éste, por esa razón las fallas están orientadas en la no afectación de la prestación del servicio.

Al hablar de proceso es necesario de acuerdo a la ISO 9001 considerar en un proceso los siguientes conceptos y elementos: [2]23

Los conceptos importantes a considerar en un proceso son:

[23] Referencia bibliográfica [9] (ISO, 2008)

- Propietarios: personas o áreas que son responsables de llevar el proceso y controlan la permanencia del mismo, también supervisa los indicadores estableciendo objetivos de mejora.
- Indicador: permite el control medible del funcionamiento del proceso, también puede servir para medir el nivel de satisfacción del usuario interno o externo.
- Cliente: son los usuarios internos o externos que utilizan la salida del proceso.

Los elementos básicos e importantes a considerar en un proceso son:

- Entrada: son elementos, personas, áreas que ponen en marcha o dan inicio al proceso, son necesarios para que el proceso pueda llevarse a cabo.
- Salidas: pueden ser productos materiales, información, recursos humanos, servicios, etc. que pueden ser utilizados para realizar alguna acción o función que tenga que hacer.
- Proceso: genera una respuesta a partir de los datos de los elementos de entrada.

En base a lo expuesto, de acuerdo a los conceptos, se define los responsables de cada proceso:

- Propietarios: O&M
- Indicador: Indicadores de Falla de los equipos de comunicaciones de ISP de acuerdo a su nivel de criticidad.

- Cliente: NOC, INGENIERÍA

A continuación detallaré los procesos que se desarrollan dentro de cada una de las funciones principales de gestión de fallas, considerando lo expuesto sobre los elementos básicos de un proceso.

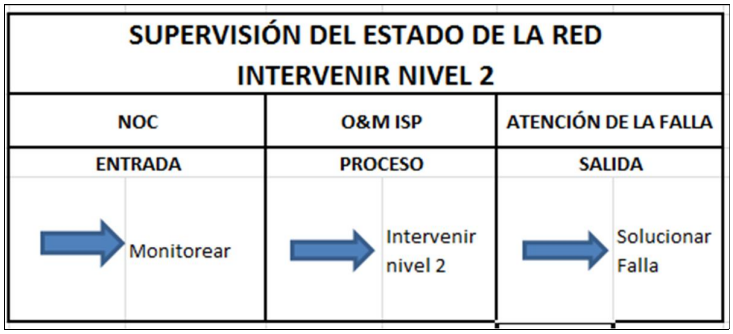
3.3.1 Supervisión del estado de la red

En la función de supervisión de la red, de acuerdo a las actividades detalladas en base a las funciones y responsabilidades de cada área y a la estructura organizacional se define la elaboración de dos procesos.

El primer proceso se desarrolla para configurar el monitoreo de los equipos de comunicaciones del ISP en la herramienta de gestión de monitoreo web CACTI, de acuerdo a los indicadores de falla, como se muestra en la gráfica 3.3.1.1.

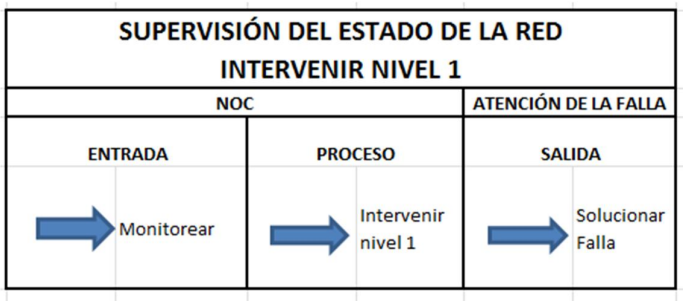
Gráfica 3.3.1.1 Proceso Supervisión del estado de la Red ï Configurar Monitoreo

El segundo proceso se desarrolla para monitorear por parte de NOC e intervenir el nivel 2 por fallas ocurridas en los equipos de comunicaciones del ISP de acuerdo a los indicadores de falla, como se muestra en la gráfica 3.3.1.2



Gráfica 3.3.1.2 Proceso Supervisión del estado de la Red ï Intervenir Nivel 2

El tercer proceso se desarrolla para monitorear por parte de NOC e intervenir el nivel 1 por fallas ocurridas en los equipos de comunicaciones del ISP de acuerdo a los indicadores de falla, como se muestra en la gráfica 3.3.1.2



Gráfica 3.3.1.3 Proceso Supervisión del estado de la Red ï Intervenir Nivel 1

Todos los procesos que corresponden a supervisión del estado de la red, están desarrollados en base a los indicadores de falla y de acuerdo a su nivel de criticidad, esto lo detallaré de mejora manera cuando se elaboren los diagramas de flujo.

3.3.2. Detección de problemas

En la función de detección de problemas, de acuerdo a las actividades detalladas en base a las funciones y responsabilidades de cada área y a la estructura

organizacional se define la elaboración de dos procesos.

El primer proceso se desarrolla para la elaborar el cronograma de mantenimiento preventivo de los equipos de comunicaciones del ISP, como se muestra en la gráfica 3.3.2.1.

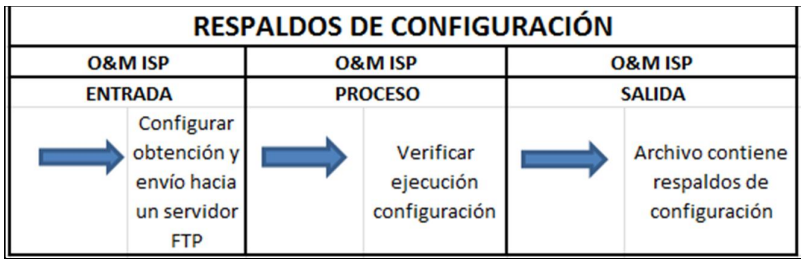
Gráfica 3.3.2.1 Proceso Detección del Problema ï Elaborar Cronograma Mantenimiento Preventivo

El segundo proceso se desarrolla para ejecutar el cronograma de mantenimiento preventivo de los equipos de comunicaciones del ISP, como se muestra en la gráfica 3.3.2.2.

Gráfica 3.3.2.2 Proceso Detección del Problema ï Ejecutar cronograma Mantenimiento Preventivo

3.3.3 Respaldos de configuración

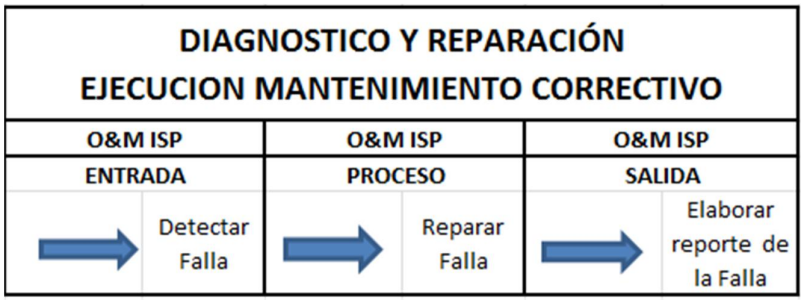
En la función de respaldos de configuración de acuerdo a las actividades detalladas en base a las funciones y responsabilidades de cada área y a la estructura organizacional se define la elaboración de un proceso, como se muestra en la gráfica 3.3.3.1.



Gráfica 3.3.3.1 Proceso Respaldos de Configuración

3.3.4 Diagnóstico y Reparación

En la función de diagnóstico y reparación, de acuerdo a las actividades detalladas en base a las funciones y responsabilidades de cada área y a la estructura organizacional se define la elaboración de un proceso, como se muestra en la gráfica 3.3.4.1.



Gráfica 3.3.4.1 Proceso Diagnóstico y Reparación ï Ejecución Mantenimiento Correctivo

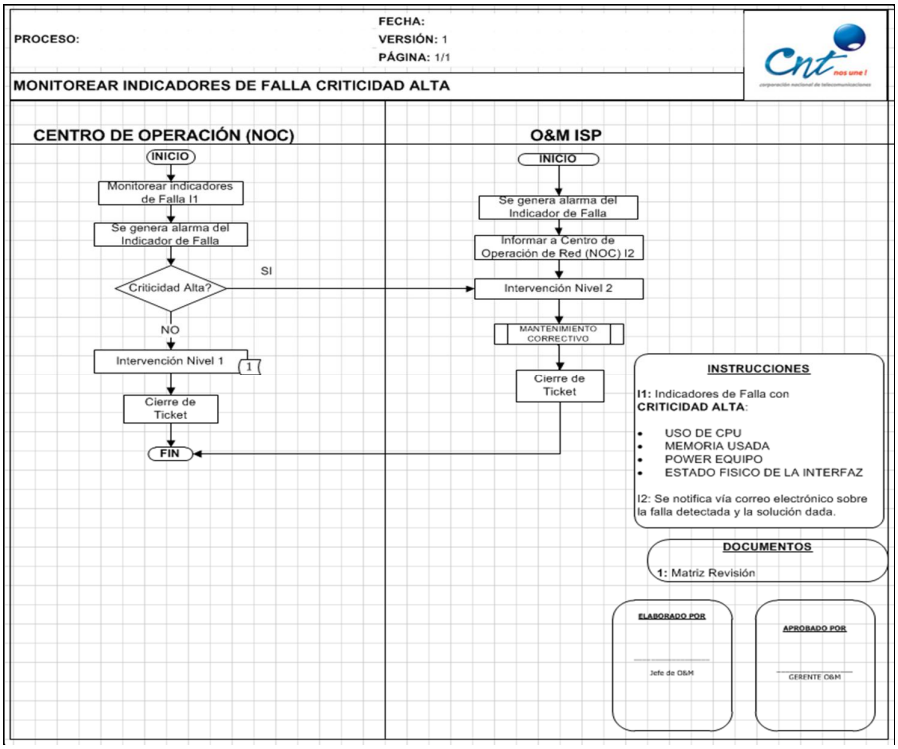
Una vez que se ha definido los procesos en cada función principal de gestión de falla entonces se procederé a elaborar el proceso en diagramas de flujo.

3.4 PROCESOS DE LAS FUNCIONES DE LA GESTION DE FALLA REPRESENTADOS EN DIAGRAMAS DE FLUJO

3.4.1 Supervisión del estado de la red

De lo expuesto anteriormente en esta función, el proceso esencial que se debe cumplir es el monitorear los indicadores de falla de acuerdo a su nivel de criticidad y atenderlos en base a los niveles de intervención.

Como podemos observar en el diagrama de flujo de la gráfica 3.4.1.1, se ha desarrollado un proceso para monitorear los indicadores de falla de acuerdo al nivel de criticidad alta, en el cual inmediatamente escala al nivel 2 para su intervención. Se ha desarrollado de esta manera el proceso ya que el impacto que puede generar la falla de este indicador puede ocasionar una indisponibilidad masiva de la prestación del servicio.



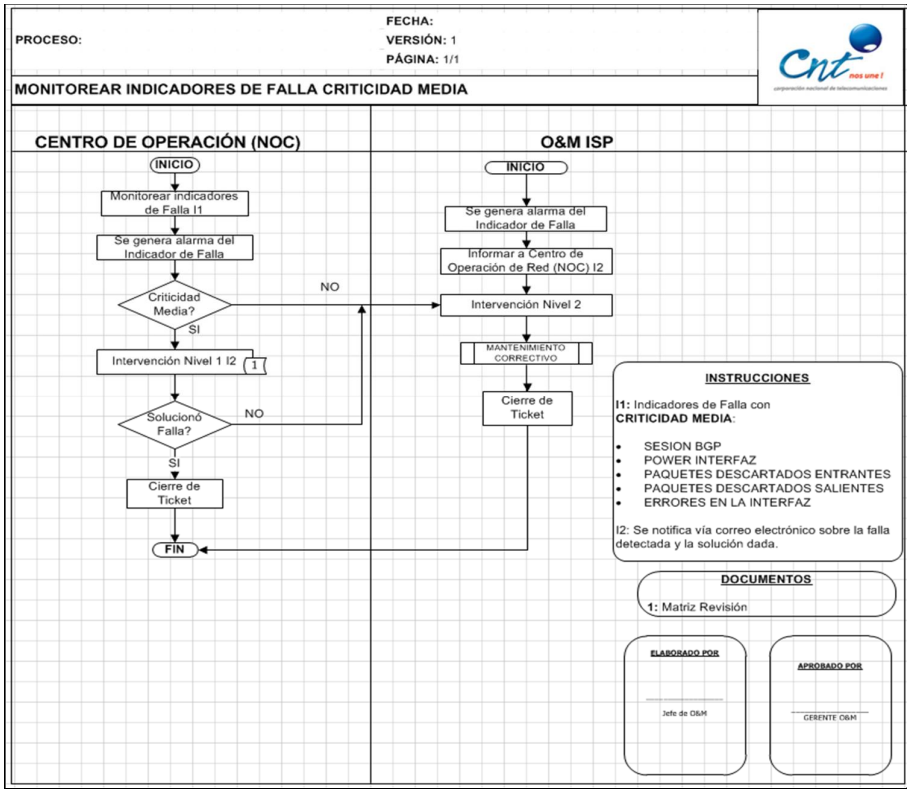
Gráfica 3.4.1.1 Monitorear Indicadores de Falla Criticidad Alta

NOC debe monitorear en la herramienta de gestión de monitoreo CACTI, los siguientes valores detallados a continuación en la Tabla 3.4.1.1 para reportar el indicador de falla.

INDICADOR	CRITICIDAD	VALORES PARA DETERMINAR UNA FALLA
USO DE CPU	ALTA	>= 85%
MEMORIA USADA	ALTA	>= 85%
POWER EQUIPO	ALTA	> carga del equipo
ESTADO FISICO DE LA INTERFAZ	ALTA	= 2

Tabla 3.4.1.1 Monitorear Indicadores de Falla Criticidad Alta ï Valores Para Reportar

En el diagrama de flujo de la gráfica 3.4.1.2 se muestra el desarrollado del proceso para monitorear los indicadores de falla de acuerdo al nivel de criticidad media, en este proceso se ha incluido como primera instancia la intervención del nivel 1 ya que se acuerdo a los indicadores el NOC con una MATRIZ REVISIÓN podría atender estas fallas, sin embargo si no logra solucionar escala al nivel 2 para su intervención. Se ha desarrollado de esta manera el proceso ya que el impacto que puede generar la falla de este indicador puede ocasionar una indisponibilidad parcial de la prestación del servicio.



Gráfica 3.4.1.2 Monitorear Indicadores de Falla Criticidad Media

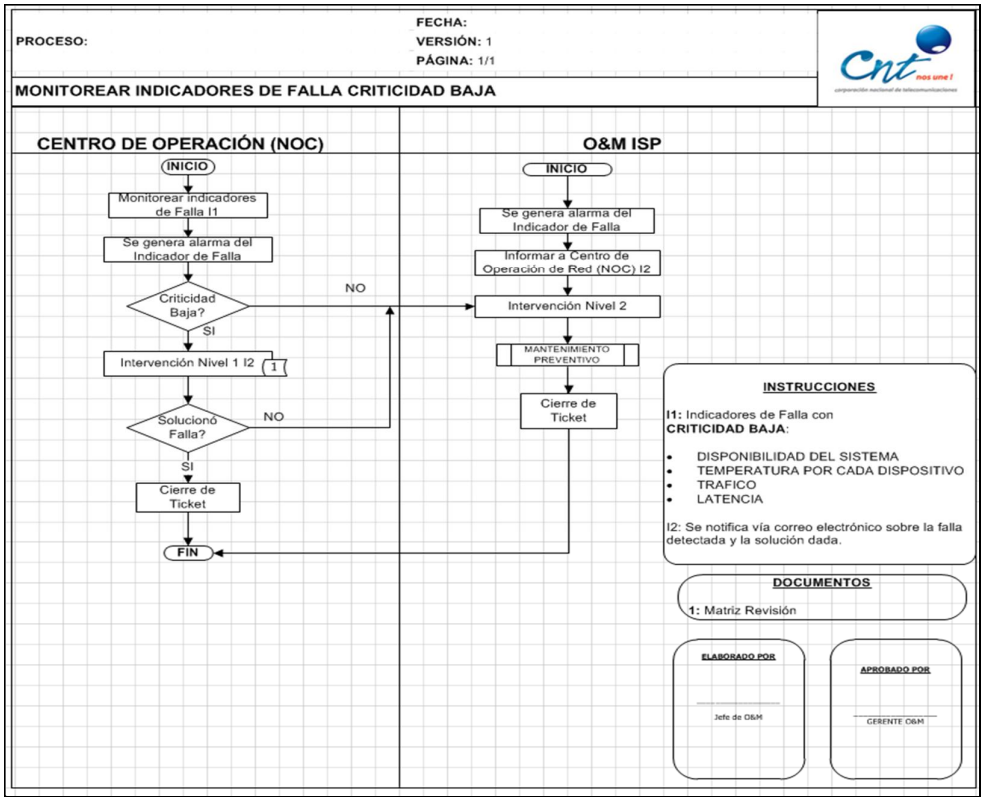
NOC debe monitorear en la herramienta de gestión de monitoreo CACTI, los

siguientes valores detallados a continuación en la Tabla 3.4.1.2 para reportar el indicador de falla.

INDICADOR	CRITICIDAD	VALORES PARA DETERMINAR UNA FALLA
SESION BGP	MEDIA	≠ 6
POWER INTERFAZ	MEDIA	> = -X dbm de la OID provista por el proveedor
PAQUETES DESCARTADOS ENTRANTES	MEDIA	> 0
PAQUETES DESCARTADOS SALIENTES	MEDIA	> 0
ERRORES EN LA INTERFAZ	MEDIA	> 0

Tabla 3.4.1.2 Monitorear Indicadores de Falla Criticidad Media ï Valores para Reportar

El diagrama de flujo de la gráfica 3.4.1.3 muestra el desarrollado del proceso para monitorear los indicadores de falla de acuerdo al nivel de criticidad baja, en este proceso también se ha incluido como primera instancia la intervención del nivel 1 ya que de acuerdo a los indicadores, el NOC con una MATRIZ REVISIÓN podría atender estas fallas, sin embargo si no logra solucionar escala al nivel 2 para su intervención. Se ha desarrollado de esta manera el proceso ya que el impacto que puede generar la falla de este indicador no ocasiona indisponibilidad masiva ni parcial de la prestación del servicio.



Gráfica 3.4.1.3 Monitorear Indicadores de Falla Criticidad Baja

Estos indicadores están orientados a realizar un análisis en ambiente de pruebas sin afectar el servicio, es decir por ejemplo, si se verifica que el up time o disponibilidad del sistema está activo desde hace un día se debe mediante mantenimiento preventivo encontrar la causa por la cual se reinició el equipo, sin embargo no se encuentra afectada la prestación del servicio, también se debe tomar en cuenta que al disponer de otro equipo o elemento redundante tampoco habría afectación en la prestación del servicio.

NOC debe monitorear en la herramienta de gestión de monitoreo CACTI, los

siguientes valores detallados a continuación en la Tabla 3.4.1.3 para reportar el indicador de falla.

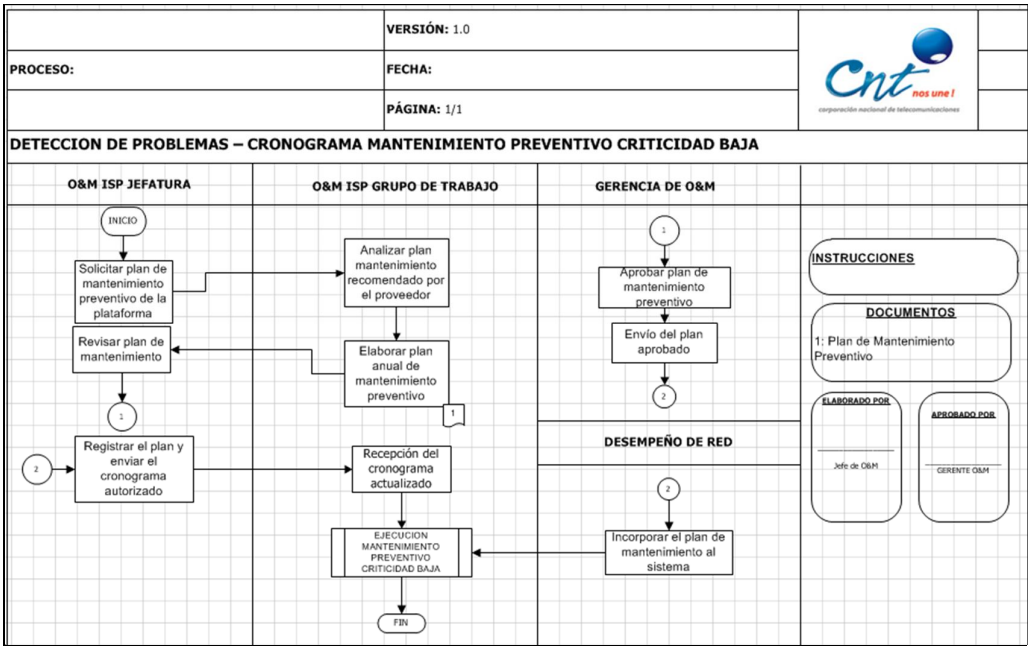
INDICADOR	CRITICIDAD	VALORES PARA DETERMINAR UNA FALLA
DISPONIBILIDAD DEL SISTEMA	BAJA	<= 1 hora
TEMPERATURA POR CADA DISPOSITIVO	BAJA	= umbral provista por el proveedor
TRAFICO	BAJA	<= 30% de la capacidad total de la interfaz
		ó > 85%
LATENCIA	BAJA	< 90 ms

Tabla 3.4.1.3 Monitorear Indicadores de Falla Criticidad Baja ï Valores para Reportar

3.4.2 Detección de problemas

En esta función de la gestión de la red se definió dos procesos, los cuales son necesarios para la detección del problema.

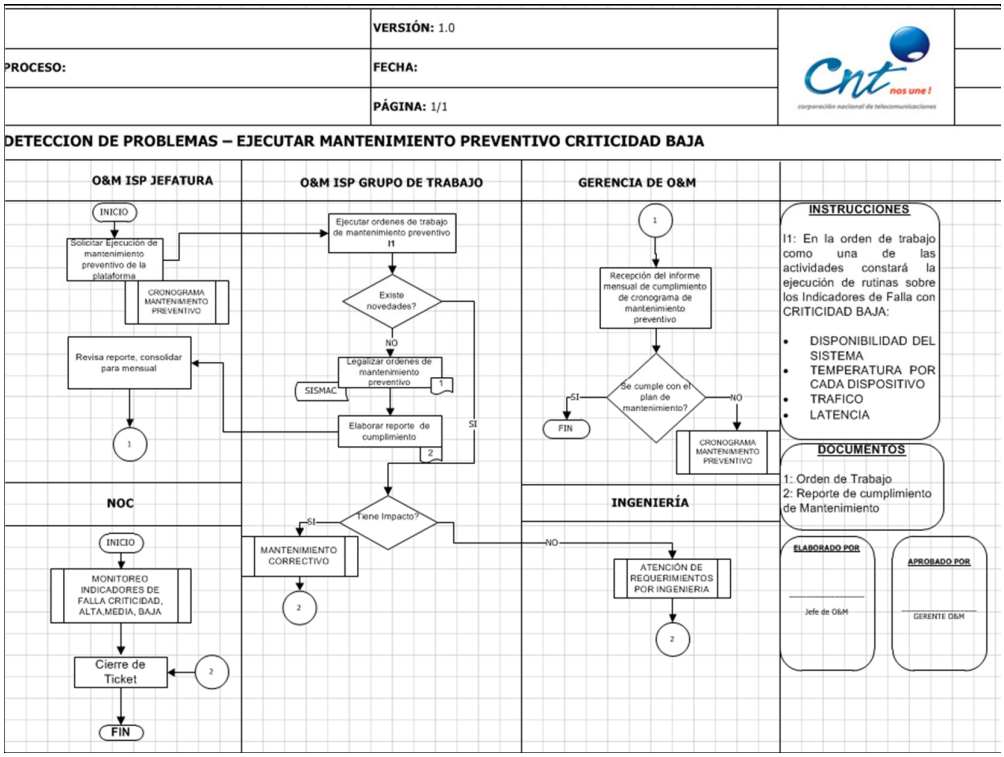
El primer diagrama de flujo que se muestra en la gráfica 3.4.2.1 detalla el proceso para elaborar y aprobar el cronograma de mantenimientos preventivos criticidad baja, está denominado así porque este proceso no implica afectación en la prestación del servicio.



Gráfica 3.4.2.1 Detección de Problemas ï Elaborar y aprobar Cronograma Mantenimiento Preventivo Criticidad Baja

Este proceso especifica el cronograma planificado para posteriormente la ejecución del mantenimiento preventivo en los equipos de comunicaciones de ISP, como se había indicado anteriormente esta actividad es importante ya que previene futuras fallas, mantiene la vida útil de un equipo y sobre todo en este proyecto apalanca los indicadores de falla de criticidad baja obtenidos anteriormente los cuales también permiten prevenir futuras fallas a nivel de la prestación del servicio.

El segundo diagrama de flujo de la gráfica 3.4.2.2 se muestra el progreso para ejecutar el cronograma de mantenimientos preventivos, en este proceso se indica, que como una de las actividades está también ejecutar rutinas sobre los indicadores de Falla clasificados con criticidad baja.



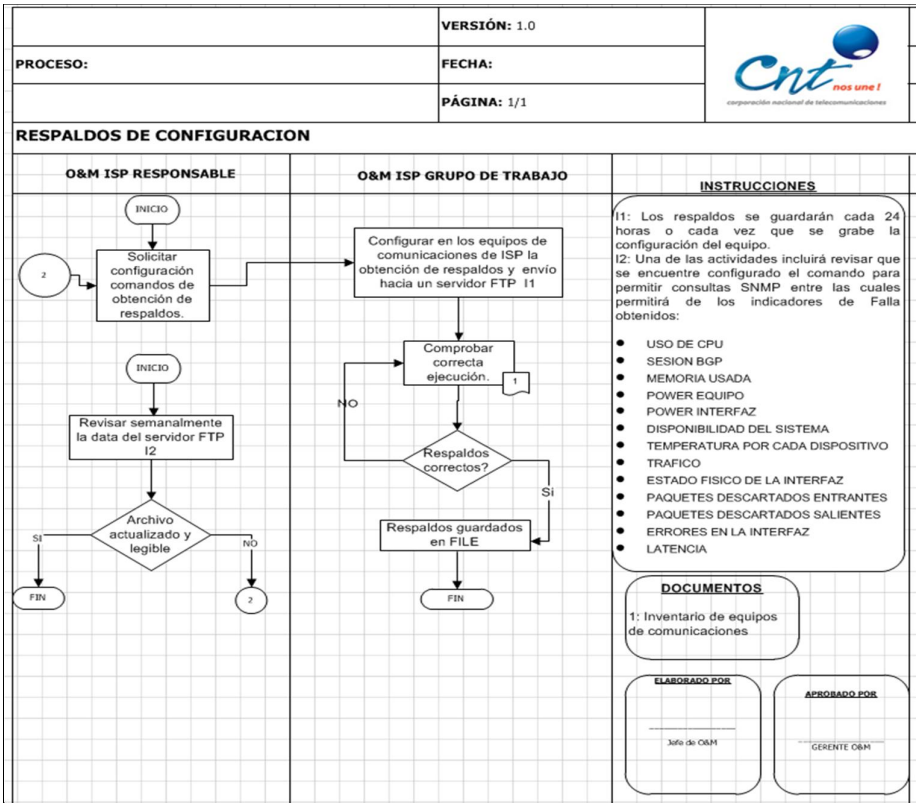
Gráfica 3.4.2.2 Detección de Problemas ï Ejecutar Cronograma Mantenimiento Preventivo Criticidad Baja

Recordando el diagrama de flujo denominado Monitoreo de Indicadores de Falla Criticidad baja, cuando NOC escala a O&M la revisión de estos indicadores, O&M lo trata dentro del proceso de mantenimiento preventivo el cual no necesariamente puede estar enfocado a cumplir la revisión con la fecha de cronograma de mantenimiento preventivo sino que también puede ser programada para una atención antes del tiempo estipulado.

3.4.3 Respaldos de configuración

En esta función de la gestión de la red se definió un proceso el cual se muestra en el

diagrama de flujo de la gráfica 3.4.3.1:



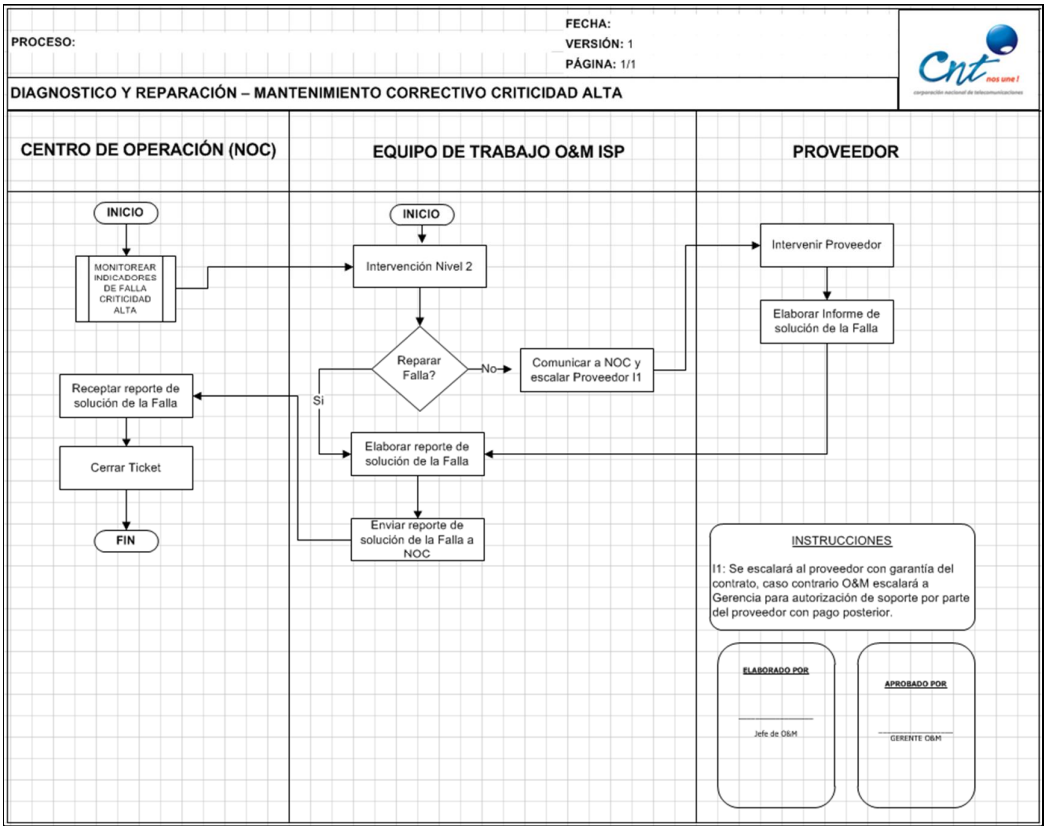
Gráfica 3.4.3.1 Respaldos de Configuración

En este proceso se debe contar con el inventario de equipos de comunicaciones de ISP para que sean configurados los mismos y se pueda obtener los respaldos de configuración. Este proceso es importante ya que si se tiene la información actualizada de la configuración de los equipos dentro de esa data se encuentra el comando que permite las consultas SNMP hacia los mismos y, al permitir éstas consultas por ende se podrá monitorear los indicadores de Falla definidos anteriormente independientes de su nivel de criticidad.

3.4.4 Diagnóstico y Reparación

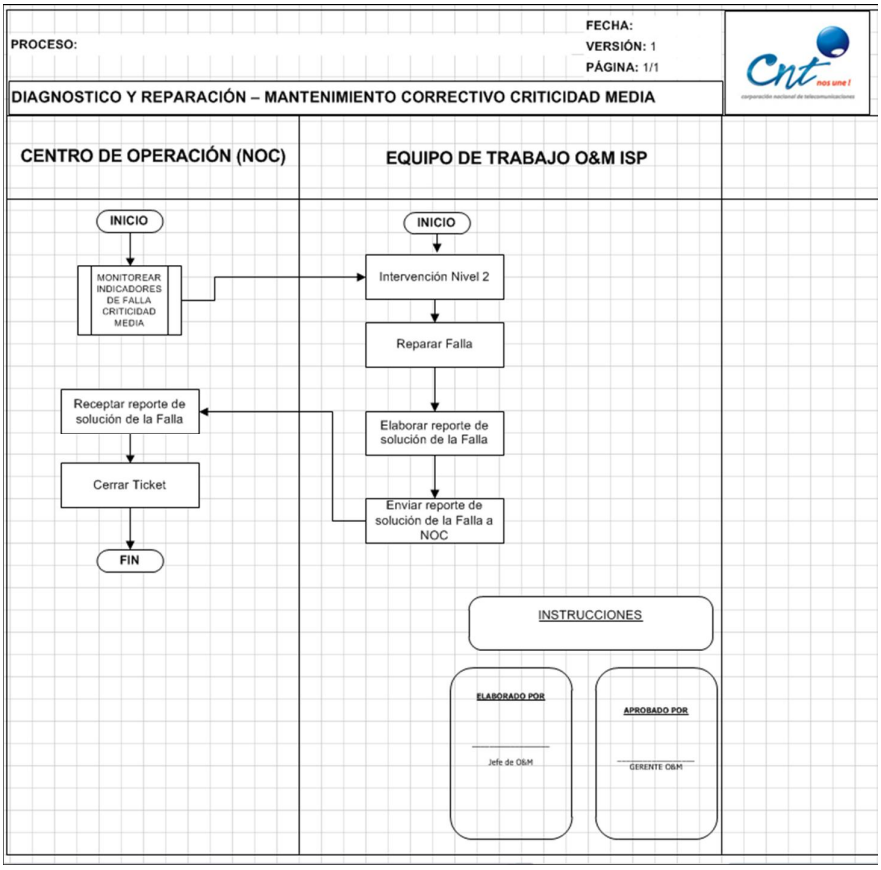
Como se puede observar en gráfica 3.4.4.1 el diagrama de flujo hace referencia a la ejecución del mantenimiento correctivo con criticidad alta, el proceso inicia con el procedimiento Monitorear indicadores de Falla Criticidad Alta por esa razón a este diagrama de flujo se lo clasificó como mantenimiento correctivo criticidad alta porque se atenderán los indicadores de falla clasificados con este nivel.

También se verifica que en este diagrama de flujo entra un área no mencionada dentro de la estructura organizacional de la empresa la cual se conoce como proveedor, los indicadores de falla descritos dentro de este proceso también pueden necesitar de la intervención del proveedor de esos equipos para la solución de los mismos por esa razón se ha colocado al proveedor dentro de este proceso aclarando que únicamente atenderá un evento de falla de un indicador si contamos con garantía técnica.



Gráfica 3.4.4.1 Diagnóstico y Reparación ï Mantenimiento Correctivo Criticidad Alta

Como se puede observar en gráfica 3.4.4.2 el diagrama de flujo hace referencia a la ejecución del mantenimiento correctivo con criticidad media, el proceso inicia con el procedimiento Monitorear indicadores de Falla Criticidad Media por esa razón a este diagrama de flujo se lo clasificó como mantenimiento correctivo criticidad media porque se atenderán los indicadores de falla clasificados con este nivel.



Gráfica 3.4.4.2 Diagnóstico y Reparación ï Mantenimiento Correctivo Criticidad Media

En el procedimiento supervisión del estado de la red, se colocó como instrucción que el 1er nivel debe realizar actividades previas antes de escalar al 2do nivel, a continuación se muestra en el Tabla 3.1.1 la MATRIZ REVISIÓN propuesta para la atención de la revisión y solución del 1er nivel de acuerdo a cada indicador de falla definido anteriormente.

INDICADOR	CRITICIDAD	QUE HACER:
USO DE CPU	ALTA	Escalar 2do Nivel
SESION BGP	MEDIA	* Validar cuales son los equipos involucrados. Esto se puede validar en el mensaje de la alarma * Confirmar si el evento se debe a un problema de Tx y si corresponde a otra área escalar y consultar a la misma sobre el evento. *Validar variaciones de tráfico en el CACTI. Escalar 2do Nivel
MEMORIA USADA	ALTA	Escalar 2do Nivel
POWER EQUIPO	ALTA	Escalar 2do Nivel
POWER INTERFAZ	MEDIA	* Validar cuales son los equipos involucrados. Esto se puede validar en el mensaje de la alarma * Validar los niveles de potencia en la interface(s) involucrada. * Confirmar si el evento se debe a un problema de energía en nodo y si corresponde a otra área escalar y consultar a la misma sobre algún evento. * Validar si existen variaciones de tráfico en el CACTI Escalar 2do Nivel
DISPONIBILIDAD DEL SISTEMA	BAJA	Se debe revisar si el último reinicio del equipo estuvo asociado a un problema anterior de no serlo Escalar 2do Nivel
TEMPERATURA POR CADA DISPOSITIVO	BAJA	* Validar cuales son los equipos involucrados. Esto se puede validar según el mensaje de la alarma * Validar la temperatura del módulo. * Validar si existe algún evento de energía en el nodo. * Validar si hay otros equipos afectados en la misma sala. * Mantener el monitoreo de la temperatura Escalar 2do Nivel
TRAFICO	BAJA	* Validar cuales son los enlaces involucrados. Esto se puede validar en el cacti. * Si la variación de tráfico es general revisar los enlaces a nivel del Backbone de Internet.

		* Si la variación de tráfico es relacionada a un nodo en particular revisar los enlaces de acceso (con las áreas relacionadas de ser el caso). Escalar 2do Nivel
ESTADO FISICO DE LA INTERFAZ	ALTA	Escalar 2do Nivel
PAQUETES DESCARTADOS ENTRANTES	MEDIA	* Realizar las revisiones del punto POWER INTERFACE. * Revisar si existen ACLs o políticas de enrutamiento para las redes afectadas. Escalar 2do Nivel
PAQUETES DESCARTADOS SALIENTES	MEDIA	* Realizar las revisiones del punto POWER INTERFACE. * Revisar si existen ACLs o políticas de enrutamiento para las redes afectadas. Escalar 2do Nivel
ERRORES EN LA INTERFAZ	MEDIA	* Realizar las revisiones del punto POWER INTERFACE. Escalar 2do Nivel
LATENCIA	BAJA	* La latencia es un parámetro que se valida origen-destino, en este sentido es importante identificar el path de referencia sobre el cual se monitorea y tener una referencia anterior (base line). * Identificar cuál de los saltos presenta variaciones (incrementos) de latencia. * Revisar interfaces saturadas o caídas. Escalar 2do Nivel

Tabla3.4.1 MATRIZ REVISION

3.5 HERRAMIENTAS Y RECURSO HUMANOS

Se considera importante definir las herramientas y recursos humanos para desarrollar las acciones descritas dentro de las funciones de Gestión de Fallas ya que son actividades que implican de personal y herramientas para cumplirlas. A continuación se considera para cada área las siguientes herramientas para cumplir con las actividades descritas anteriormente en los flujogramas.

O&M

- Servidores con mouse, pantalla, para configurar CACTI con sus respectivos monitoreos.
- Lugar Físico para colocar estos equipos.
- Estación de trabajo para el personal.
- Línea telefónica

NOC

- Computadores con mouse, pantalla, para cargar URL CACTI con sus respectivos monitoreos.
- Lugar Físico para colocar estos equipos.
- Estación de trabajo para el personal.
- Línea telefónica

INGENIERIA

- Computadores con mouse, pantalla, para cargar URL CACTI con sus respectivos monitoreos.
- Lugar Físico para colocar estos equipos.
- Estación de trabajo para el personal.
- Línea telefónica

DESEMPEÑO

- Computadores con mouse, pantalla, para cargar URL CACTI con sus respectivos monitoreos.
- Lugar Físico para colocar estos equipos.
- Estación de trabajo para el personal.
- Línea telefónica

GERENCIA

- Computadores con mouse, pantalla, para cargar URL CACTI con sus respectivos monitoreos.
- Lugar Físico para colocar estos equipos.
- Estación de trabajo para el personal.
- Línea telefónica

Para el cálculo del personal se ha elaborado una matriz en Excel la cual consta del proceso, actividades, demanda, duración. En esta tabla se ha colocado valores mínimos y máximos de acuerdo a la demanda únicamente para referencia, el cálculo se lo realiza entre la demanda mensual y la duración por la demanda y las horas hombres corresponderían a este valor. Ahora para conocer el total de personas que se requiere para la N cantidad de horas hombres simplemente se divide para la multiplicación de 8 horas laborables por los cinco días de la semana y por las 4 semanas que dura el mes. Es así que a continuación se mostrará las

gráficas en las cuales indicará cuanto personal se requiere para realizar estas actividades en cada área.

La Gráfica 3.5.1 muestra la matriz con las actividades detalladas en cada función de la Gestión de Fallas y que deben realizarse por parte del grupo O&M.

Como se puede observar la cantidad de personas que se requiere para realizar estas actividades durante el mes es de 5.

ANÁLISIS RECURSO HUMANOS REQUERIDO GESTION DE FALLAS										
		DEMANDA			DURACION (en minutos)					
PROCESO	ACTIVIDAD	MIN	MODA	MAX	MIN	MODA	MAX	AREA	HORAS HOMBRE	
Supervisión y estado de la Red	Configuración del monitoreo en CACTI de los equipos de comunicaciones de ISP de acuerdo a los indicadores de falla	11	14	16,8	672	840	1008	ACTIVIDADES O&M	196,0	
	Intervenir nivel 2	4,8	6	7,2	432	540	648		54,0	
Detección de Problemas	Elaborar cronograma de mantenimiento preventivo.	0,8	1	1,2	48	60	72	ACTIVIDADES O&M	1,0	
	Solicitar Aprobación a la Gerencia O&M	0,8	1	1,2	48	60	72		4,0	
	Ejecución Mantenimiento preventivo	3,2	4	4,8	576	720	864		48,0	
	Elaborar Reporte de cumplimiento mensual	3,2	4	4,8	192	240	288		16,0	
Respaldos de Configuración	Solicitar configuración de los comandos de obtención de respaldos.	3,2	4	4,8	48	60	72	ACTIVIDADES O&M	4,0	
	Configurar en los equipos de comunicaciones de ISP la obtención de los respaldos de la configuración y envío hacia un servidor FTP cada 12 horas. Comprobar correcta ejecución.	9,6	12	14,4	576	720	864		144,0	
	Configurar en los equipos de comunicaciones de ISP la obtención los respaldos dela configuración y envío hacia un servidor FTP cada vez que se grabe la configuración. Comprobar correcta ejecución.	9,6	12	14,4	576	720	864		144,0	
	Revisar semanalmente que la data del servidor FTP esté actualiza con el último archivo guardado y validar que sea legible.	3,2	4	4,8	192	240	288		16,0	
Diagnóstico y Reparación	Diagnosticar o detectar la Falla.	4	5	6	240	300	360	ACTIVIDADES O&M	25,0	
	Reparar la Falla	4	5	6	720	900	1080		75,0	
	Elaborar informe de solución de la Falla	4	5	6	360	450	540		37,5	
	Enviar informe de la solución de la Falla a NOC	4	5	6	240	300	360		25,0	
									789,5	5

Gráfica 3.5.1 Cantidad de personal O&M para cumplir Gestión de Fallas

La Gráfica 3.5.2 muestra la matriz con las actividades detalladas en cada función de la Gestión de Fallas y que deben realizarse por parte del grupo NOC.

Como se puede observar la cantidad de personas que se requiere para realizar estas actividades durante el mes es de 2.

ANÁLISIS RECURSO HUMANOS REQUERIDO GESTION DE FALLAS									
		DEMANDA			DURACION (en				
PROCESO	ACTIVIDAD	MIN	MODA	MAX	MIN	MODA	MAX	AREA	HORAS HOMBRE
Supervisión y estado de la Red	Monitorear Indicadores de Falla de acuerdo a su nivel de criticidad, valor y MATRIZ REVISIÓN	11	14	16,8	1008	1260	1512	ACTIVIDADES NOC	294,0
	Intervenir nivel 1	6,4	8	9,6	384	480	576	ACTIVIDADES NOC	64,0
									358,0 2

Gráfica 3.5.2 Cantidad de personal NOC para cumplir Gestión de Fallas

La Gráfica 3.5.3 muestra la matriz con las actividades detalladas en cada función de la Gestión de Fallas y que deben realizarse por parte del grupo INGENIERIA.

Como se puede observar la cantidad de personas que se requiere para realizar estas actividades durante el mes es de 1.

ANÁLISIS RECURSO HUMANOS REQUERIDO GESTION DE FALLAS									
		DEMANDA			DURACION (en minutos)				
PROCESO	ACTIVIDAD	MIN	MODA	MAX	MIN	MODA	MAX	AREA	HORAS HOMBRE
Detección de Problemas	Verificar y analizar requerimiento de mejora o ampliación	8	10	12	576	720	864	ACTIVIDADES INGENIERIA	120,0
	Generar Orden de Trabajo	8	10	12	192	240	288		40,0
									160,0 1

Gráfica 3.5.3 Cantidad de personal INGENIERIA para cumplir Gestión de Fallas

La Gráfica 3.5.4 muestra la matriz con las actividades detalladas en cada función de la Gestión de Fallas y que deben realizarse por parte del grupo DESEMPEÑO.

Como se puede observar la cantidad de personas que se requiere para realizar estas actividades durante el mes es de 1.

ANÁLISIS RECURSO HUMANOS REQUERIDO GESTION DE FALLAS										
		DEMANDA			DURACION (en minutos)					
PROCESO	ACTIVIDAD	MIN	MODA	MAX	MIN	MODA	MAX	AREA	HORAS HOMBRE	
Detección de Problemas	Registrar Orden de Trabajo	8	10	12	192	240	288	ACTIVIDADES DESEMPEÑO	40,0	
	Gestionar Cambios	8	10	12	192	240	288		40,0	
	Incorporar el plan de mantenimiento en el sistema.	8	10	12	192	240	288		40,0	
									120,0	1

Gráfica 3.5.4 Cantidad de personal DESEMPEÑO para cumplir Gestión de Fallas

La Gráfica 3.5.4 muestra la matriz con las actividades detalladas en cada función de la Gestión de Fallas y que deben realizarse por parte del grupo GERENCIA.

Como se puede observar la cantidad de personas que se requiere para realizar estas actividades durante el mes es de 0.

ANÁLISIS RECURSO HUMANOS REQUERIDO GESTION DE FALLAS										
		DEMANDA			DURACION (en minutos)					
PROCESO	ACTIVIDAD	MIN	MODA	MAX	MIN	MODA	MAX	AREA	HORAS HOMBRE	
Detección de Problemas	Aprobar cronograma de mantenimiento preventivo	3,2	4	4,8	192	240	288	ACTIVIDADES GERENCIA O&M	16,0	
	Verificar cumplimiento	3,2	4	4,8	192	240	288		16,0	
									32,0	0

Gráfica 3.5.5 Cantidad de personal GERENCIA para cumplir Gestión de Fallas

De acuerdo al análisis realizado sobre el recurso humano, en la Tabla3.5 se resumen la cantidad de recurso Humano requerido por cada área para cumplir con las actividades de las funciones de Gestión de Fallas.

AREA	RECURSO HUMANO REQUERIDO
O&M	5
NOC	2
INGENIERIA	1
DESEMPEÑO	1

Tabla3.5 Cantidad de Recurso Humano requerido

4. CAPITULO IV – APLICAR EL PROCESO DEL MODELO A UN GRUPO DE FALLAS

4.1 PROCEDIMIENTO

En el capítulo III se clasificó los indicadores de falla que se pueden obtener mediante la herramienta de gestión de monitoreo CACTI, a este listado de indicadores de acuerdo al impacto de afectación de la prestación del servicio se los clasificó con un nivel de criticidad y también se definió un valor para reportar el indicador de Falla. Dentro de la metodología de atención de fallas de acuerdo a las funciones principales de gestión de fallas se desarrolló los procedimientos relacionados con cada una de ellas y se definió que procesos intervienen en los mismos.

También se definió las responsabilidades al interior de la organización necesaria para poner en marcha el modelo de gestión, de tal forma que la agrupación de las diferentes medidas de acción encontradas para el mismo, permitan determinar proyectos o planes de acción y asignar las responsabilidades y objetivos al interior de la organización.

Los diagramas de flujo establecen una herramienta muy útil para describir los procesos, es decir, indican el procedimiento a seguir en cada uno de ellos ya que permiten explicar de mejor manera las actividades y las áreas involucradas, CNT EP

los utiliza y son registrados en su plataforma oficial de información (MAI) de procesos.

El procedimiento implementado para los procesos de gestión de fallas está representado en cada diagrama de flujo correspondiente a cada función de la gestión de falla desarrollada en el Capítulo III.

4.2 PLANIFICACIÓN DE LA ATENCIÓN DE FALLAS

Para la planificación de atención de fallas previamente se formó los procesos del capítulo III. Cada proceso desarrollado dentro de cada función tiene una organización enfocada a la atención de fallas de los indicadores definidos, a continuación detallaré el listado de procesos de las funciones de la gestión de Falla que fueron representados en diagramas de flujo los cuales se aplicarán para la planificación de la atención de Fallas. Cabe acotar que dentro de cada flujograma del proceso se definió el valor del indicador de falla para reportar.

- Supervisión del estado de la red
    - Monitorear Indicadores de Falla Criticidad Alta
    - Monitorear Indicadores de Falla Criticidad Media
    - Monitorear Indicadores de Falla Criticidad Baja

- Detección de problemas

- Elaborar y aprobar Cronograma Mantenimiento Preventivo
- Ejecutar Cronograma Mantenimiento Preventivo

- Respaldos de Configuración
  - Respaldos de Configuración

- Diagnóstico y Reparación
  - Mantenimiento Correctivo Criticidad Alta
  - Mantenimiento Correctivo Criticidad Media

4.3 IMPLEMENTACIÓN

En este ITEM se ensayará verificar la lógica de los procesos definidos para la Gestión de Fallas de los equipos de comunicaciones del ISP mediante un seguimiento a los flujos de actividades de cada proceso desarrollado en el capítulo III y representados mediante sus correspondientes diagramas de flujo, para este ensayo se tomará como muestra algunos equipos de comunicaciones del ISP y se realizará el ensayo para todos los indicadores de falla definidos.

De acuerdo a lo detallado en el ITEM anterior procederé a realizar un ensayo de cada función de la gestión de falla.

- **Para el proceso Supervisión del estado de la red.**

Para esta función de desarrolló tres procesos:

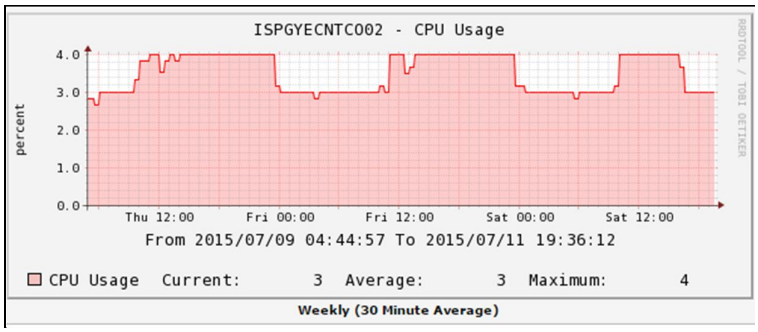
Monitorear Indicadores de Falla Criticidad Alta

Este proceso se desarrolló para monitoreo de los siguientes indicadores de falla:

- **USO DE CPU**

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla "USO DE CPU" del equipo de comunicaciones de ISP Core Guayaquil el cual fue previamente definido, este monitoreo fue tomado durante el periodo de dos días.



Gráfica 4.1.1 Monitoreo indicador de Falla - USO CPU

Como se puede observar en la gráfica 4.1.1 se tiene de tres a 4 % de USO de CPU del total del 100%, de acuerdo al valor que se muestra en la Tabla3.1.2 del capítulo III (>= 85%), no es igual ni supera el 85% para reportar una falla, encontrándose

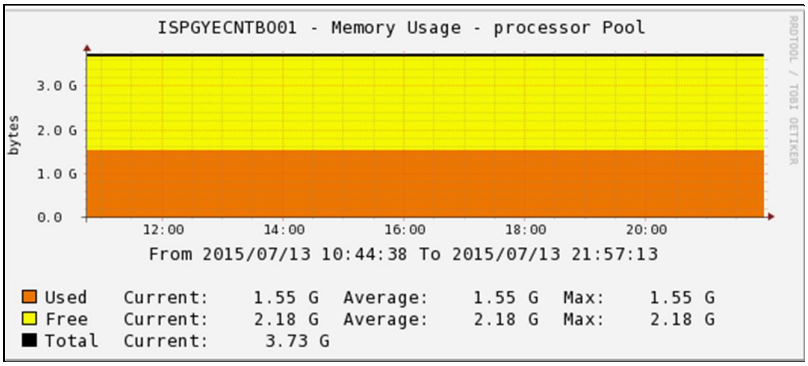
normal.

- *Se genera alarma del Indicador de Falla*: NO.
- *Toma de Decisión:* Criticidad Alta?
    - SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

- **MEMORIA USADA**

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla "MEMORIA USADA" del equipo de comunicaciones de ISP Borde Guayaquil, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.2 Monitoreo indicador de Falla ï MEMORIA USADA

Como se puede observar en la gráfica 4.1.2 se tiene 1.55G de USO de MEMORIA del

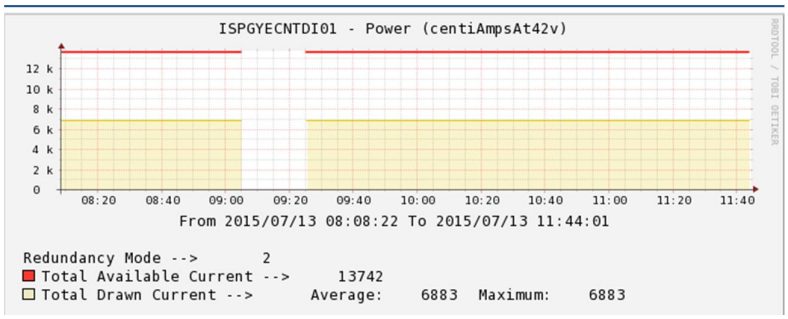
total de 3.73G por lo que no es igual ni supera el 85%, valor que se muestra en la Tabla3.1.2 del capítulo III (>=85%) para reportar una falla, encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Alta?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

- **POWER EQUIPO**

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla "POWER EQUIPO" del equipo de comunicaciones de ISP Distribución Guayaquil, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.3 Monitoreo indicador de Falla ï POWER EQUIPO

Como se puede observar en la gráfica 4.1.3 muestra 6883 de USO de AMPERIOS del total de la carga que soporta el equipo la cual corresponde a 13742 por lo que no es mayor al valor total de acuerdo al valor que se muestra en la Tabla3.1.2 del capítulo III (> carga del equipo) para reportar una falla, encontrándose normal. Sin embargo existe un corte en la gráfica a las 09:00 hasta las 09:20. Se verifica logs del equipo no se encuentra ningún problema se verifica el monitoreo y se identifica que no graficó durante ese periodo se realiza afinamiento.

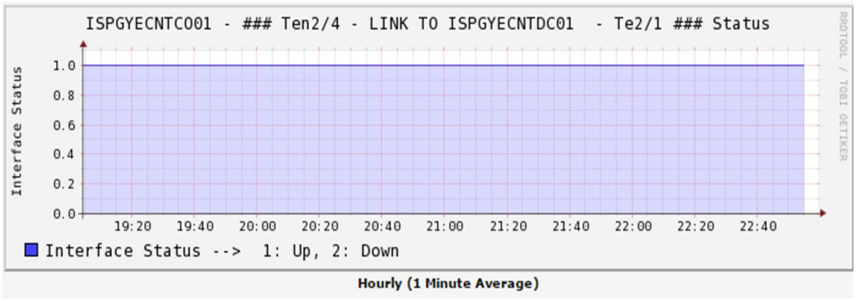
- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Alta?*
    - *SI: a pesar de que no existe alarma del indicador de falla pero hay un corte en la gráfica se escala Intervención Nivel 2.*
- Intervención Nivel 2: personal de OM ejecuta proceso de mantenimiento correctivo detectando y solucionando problema del monitoreo CACTI el cual debido a que se encuentra en un servidor virtual perdió conectividad.
- Cierre de Ticket.

    - **ESTADO FISICO DE LA INTERFAZ**

- **Monitorear indicadores de Falla:**

NOC monitorea el indicador de falla “ESTADO FISICO DE LA INTERFAZ” entre los

equipos de comunicaciones de ISP Distribución y Core de Guayaquil, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de 3 horas.



Gráfica 4.1.4 Monitoreo indicador de Falla ï
ESTADO FISICO DE LA INTERFAZ

Como se puede observar en la gráfica 4.1.4 el indicador de Falla se encuentra UP=1, por lo que no es igual al valor que se muestra en la Tabla3.1.2 del capítulo III (= 2) para reportar una falla encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Alta?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

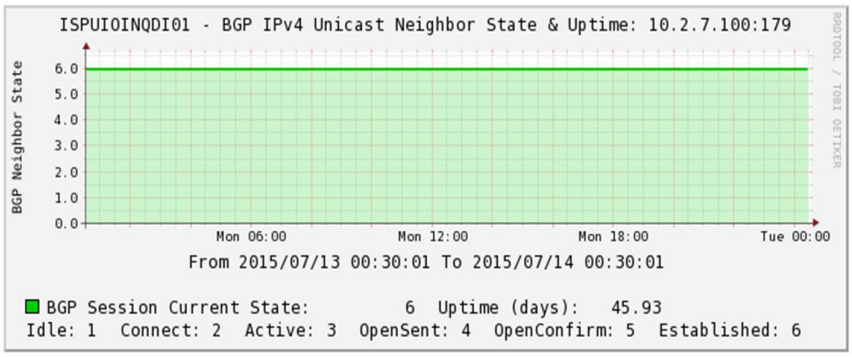
Monitorear Indicadores de Falla Criticidad Media

Este proceso se desarrolló para monitoreo de los indicadores de falla siguientes:

- **SESION BGP**

- **Monitorear indicadores de Falla:**

NOC monitorea el indicador de falla "SESION BGP" del equipo de comunicaciones de ISP Distribución Quito, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.5 Monitoreo indicador de Falla ï SESION BGP

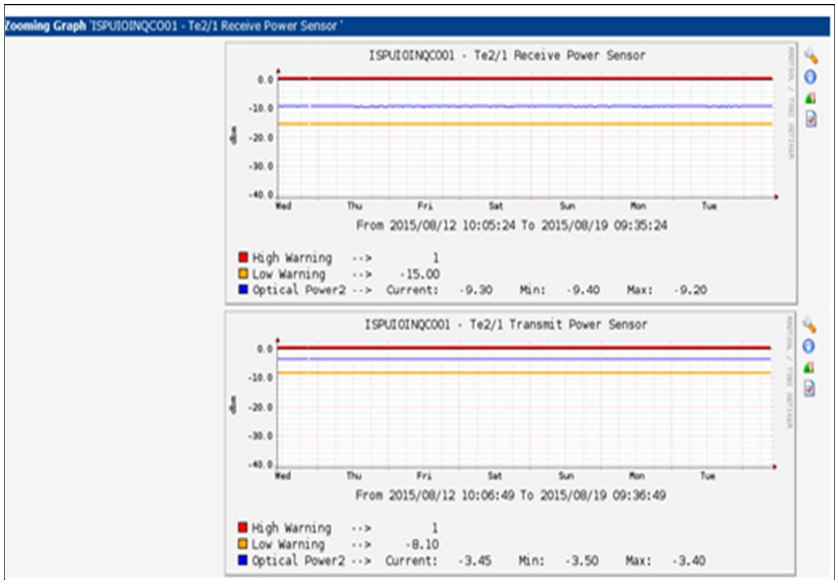
Como se puede observar en la gráfica 4.1.5 el indicador de Falla muestra el proceso del establecimiento de la sesión BGP = 6, e indica el número de días que se encuentra activa la misma para este ejemplo son 45.93 días, por lo que no es un valor diferente al valor que se muestra en la Tabla3.1.2 del capítulo III (≠ 6) para reportar una falla encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Media?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

- **POWER INTERFAZ**

- **Monitorear indicadores de Falla:**

NOC monitorea el indicador de falla “POWER INTERFAZ” que hace referencia a la potencia óptica de la interfaz Te2/1 del equipo de comunicaciones de ISP Core Quito, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.6 Monitoreo indicador de Falla ï POWER INTERFAZ

Como se puede observar en la gráfica 4.1.6 los valores de corriente de la interfaz de acuerdo al valor obtenido en CACTI tienen valores en la recepción -9.30 dbm y en la transmisión -3.45 dbm, también se puede observar el valor que toma como umbral el equipo para reportar una falla por ejemplo en la interfaz de recepción es = -15dbm, y en la interfaz de transmisión es = -8.10 dbm, entonces estos valores actuales de la potencia óptica no son iguales o menores a los del umbral del equipo por lo cual no igualan a los valores que se muestra en la Tabla3.1.2 del capítulo III (> = -X dbm de la OID provista por el proveedor) para reportar una falla, encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Media?*

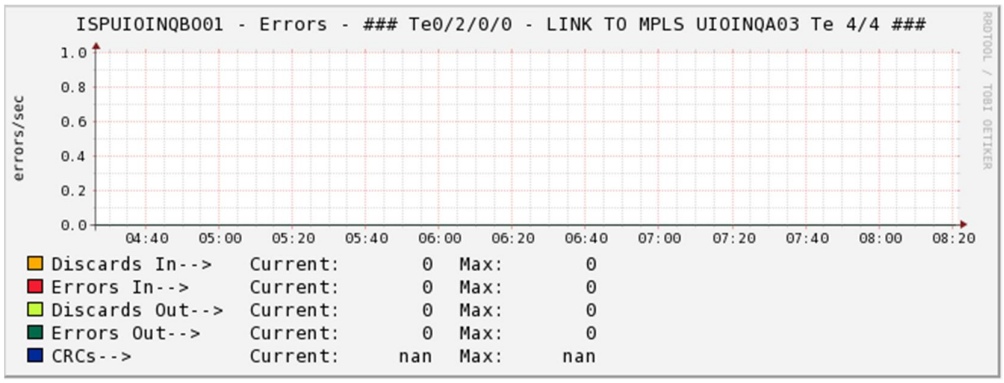
- *SI: No hay alarma del indicador de falla como no hay alarma del indicador no se escala a nivel 2. Entonces Intervención Nivel 1.*

- *Toma de Decisión: Solucionó Falla?*
  - *SI: No hay alarma del indicador de falla, no hubo falla.*
- Cierre de Ticket.

- **PAQUETES DESCARTADOS ENTRANTES**

- **Monitorear indicadores de Falla:**

NOC monitorea el indicador de falla "PAQUETES DESCARTADOS ENTRANTES" del equipo de comunicaciones de ISP Borde de Quito, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de 4 horas.



Gráfica 4.1.7 Monitoreo indicador de Falla ï
PAQUETES DESCARTADOS ENTRANTES

Como se puede observar en la gráfica 4.1.7 no se ha mostrado paquetes descartados entrantes en la interfaz del borde que se conecta con el equipo MPLS

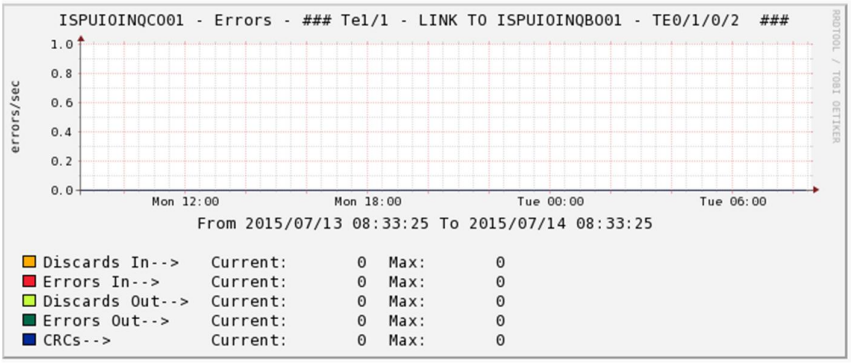
ya que se tiene 0 descartados por segundo, por lo que no supera el valor que se muestra en la Tabla3.1.2 del capítulo III (> 0) para reportar una falla encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Media?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

- **PAQUETES DESCARTADOS SALIENTES**

- **Monitorear indicadores de Falla:**

NOC monitorea el indicador de falla “PAQUETES DESCARTADOS SALIENTES” de los equipos de comunicaciones de ISP Borde y Core de Quito, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.8 Monitoreo indicador de Falla ï
PAQUETES DESCARTADOS SALIENTES

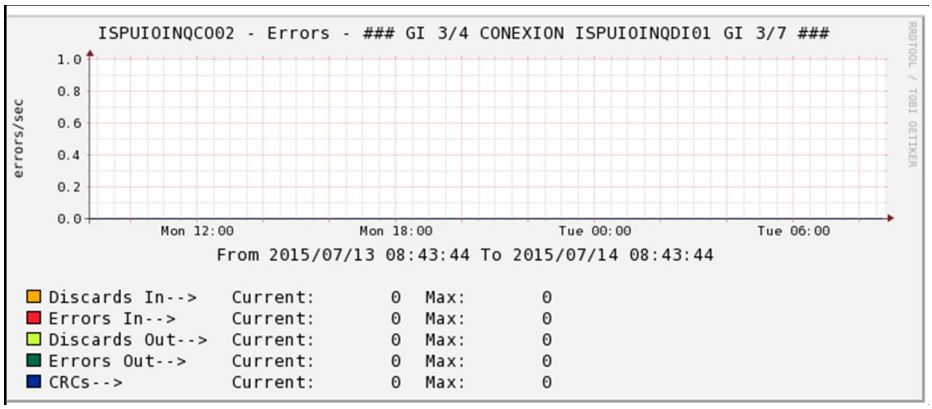
Como se puede observar en la gráfica 4.1.8 no se ha mostrado paquetes descartados salientes en la interfaz del borde que se conecta con el equipo Core ya que se tiene 0 descartados por segundo, por lo que no supera el valor que se muestra en la Tabla3.1.2 del capítulo III (> 0) para reportar una falla encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Media?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

- **ERRORES EN LA INTERFAZ**

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla “ERRORES EN LA INTERFAZ” de los equipos de comunicaciones de ISP Core y Distribución de Quito, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.9 Monitoreo indicador de Falla ï
ERRORES EN LA INTERFAZ

Como se puede observar en la gráfica 4.1.8 no se ha mostrado errores en la interfaz del core que se conecta con el equipo distribución ya que se tiene 0 errores por segundo, por lo que no supera el valor que se muestra en la Tabla3.1.2 del capítulo III (> 0) para reportar una falla encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*

- *Toma de Decisión: Criticidad Media?*

  - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*

- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

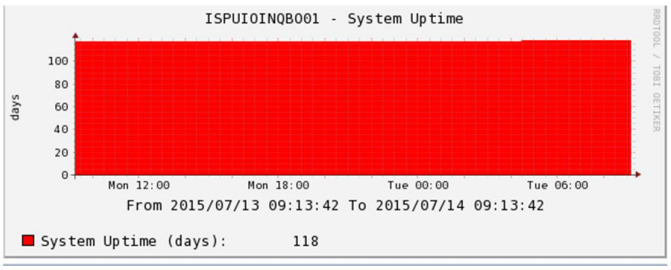
Monitorear Indicadores de Falla Criticidad Baja

Este proceso se desarrolló para monitoreo de los indicadores de falla siguientes:

- **DISPONIBILIDAD DEL SISTEMA**

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla "DISPONIBILIDAD DEL SISTEMA" del equipo de comunicaciones de ISP Borde Quito, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.10 Monitoreo indicador de Falla ï DISPONIBILDIAD DEL SISTEMA

Como se puede observar en la gráfica 4.1.10 el indicador de Falla muestra el tiempo que el equipo permaneció encendido indicando que el número de días que se encuentra sin reiniciarse para este ejemplo son 118 días, por lo cual el valor no es menor o igual al valor que se muestra en la Tabla3.1.2 del capítulo III (<= 1 hora)

para reportar una falla, encontrándose normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Baja?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.
    - **TEMPERATURA POR CADA DISPOSITIVO**
- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla “TEMPERATURA POR CADA DISPOSITIVO” del equipo de comunicaciones de ISP Distribución Guayaquil, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de 11 días.

Gráfica 4.1.11 Monitoreo indicador de Falla ï
TEMPERATURA POR CADA DISPOSITIVO

Como se puede observar en la gráfica 4.1.11 muestra la temperatura de la tarjeta procesadora del equipo de Distribución de Guayaquil la cual indica el valor en Celsius de la entrada y salida siendo 25 y 29 respectivamente, también indica el valor del umbral para ambos casos 65 Celsius, de acuerdo a la Tabla3.1.2 del capítulo III (= umbral provista por el proveedor) el valor para reportar una falla tiene que ser igual al umbral definido por el proveedor del equipo, en este caso no el igual por lo que la temperatura se encuentra normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Baja?*
    - *SI: No hay alarma del indicador de falla por lo que no*

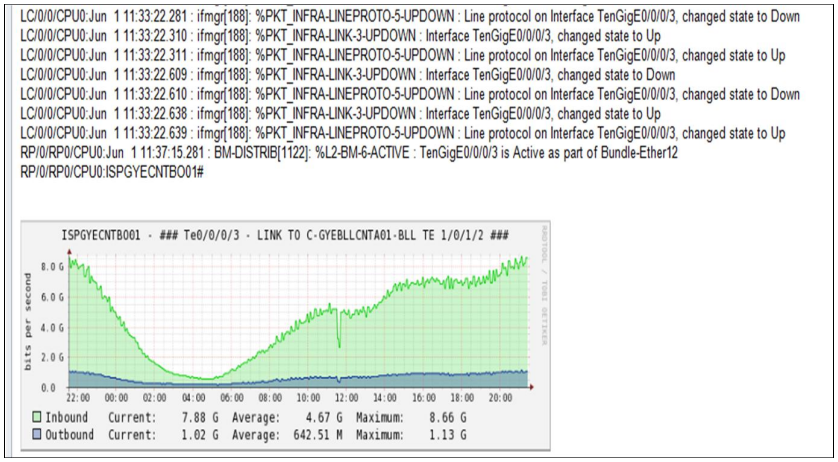
se escala a nivel 2.

- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

o TRAFICO

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla "TRAFICO" del equipo de comunicaciones de ISP Borde Guayaquil, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de un día.



Gráfica 4.1.12 Monitoreo indicador de Falla ï TRAFICO

Como se puede observar en la gráfica 4.1.12 se puede evidenciar que existen bajas de tráfico igual al 30% de la capacidad total de la interfaz lo cual de acuerdo a los logs del equipo fue ocasionado por un flapeo a nivel de protocolo en la interfaz

Te0/0/0/3 del equipo Borde de Guayaquil que se conecta hacia un equipos MPLS mediante una TX de Fibra Óptica.

NOC confirma con el área de transmisiones que tuvieron eventos en la fibra y al empalmar ocasionaron estos flapeos. Por lo indicado concuerda con el valor que se muestra en la Tabla3.1.2 del capítulo III (<=30% de la capacidad total de la interfaz) para reportar una falla.

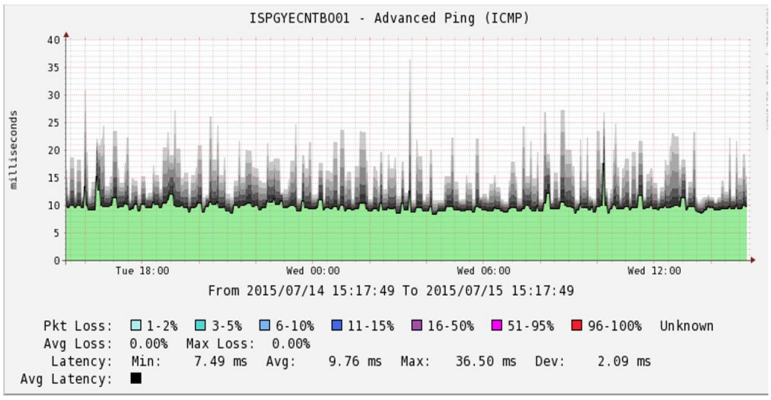
- *Se genera alarma del Indicador de Falla: SI.*
- *Toma de Decisión: Criticidad Baja?*
    - *SI: Hay reporte del indicador de falla.*
- Intervención Nivel 1: Hay intervención del Nivel1 para revisar la causa de la baja de tráfico. Corte de Fibra por el área de Transmisiones lo cual ocasiona flapeos durante los trabajos de empalme.
- *Solucionó Falla? SI*
- El tráfico se recupera luego de las acciones tomadas por el área de Transmisiones.
- Cierre de Ticket.

- **LATENCIA**

- Monitorear indicadores de Falla:

NOC monitorea el indicador de falla “LATENCIA” del equipo de comunicaciones de

ISP Borde Guayaquil, el cual fue previamente definido, este monitoreo fue tomado durante el periodo de 1 día.



Gráfica 4.1.13 Monitoreo indicador de Falla ï LATENCIA

Como se puede observar en la gráfica 4.1.13 el indicador de Falla muestra el tiempo mínimo, máximo, promedio de respuesta de ping entonces el tiempo de respuesta promedio esta sobre los 9.76 ms, revisado el valor que se muestra en la Tabla3.1.2 del capítulo III (<=90ms) para reportar una falla, la latencia está normal.

- *Se genera alarma del Indicador de Falla: NO.*
- *Toma de Decisión: Criticidad Baja?*
    - *SI: No hay alarma del indicador de falla por lo que no se escala a nivel 2.*
- Intervención Nivel 1: como no se generó falla del indicador NO hay intervención del Nivel1.
- Cierre de Ticket.

- **Detección de Problemas.**

  Para esta función de desarrolló dos procesos:

Elaborar y Aprobar Cronograma Mantenimiento Preventivo Criticidad Baja

- O&M ISP JEFATURA

- *Solicitar plan de mantenimiento preventivo de la plataforma:*

  La jefatura solicita al grupo de trabajo el plan de mantenimiento.

- O&M ISP GRUPO DE TRABAJO

- *Analizar plan de mantenimiento recomendado por el proveedor:*

  El grupo de trabajo de O&M revisa el plan de mantenimiento propuesto por el proveedor acoge algunas recomendaciones y coloca dentro de las actividades la de ejecutar también las rutinas de los indicadores de falla con criticidad baja.

- *Elaborar plan anual de mantenimiento preventivo*

  El grupo de O&M elabora el plan de mantenimiento preventivo y envía a la jefatura para revisión y aprobación.

- O&M ISP JEFATURA

- *Revisar plan de mantenimiento:*

  La jefatura revisa el plan y si está de acuerdo a las políticas internas de CNT

se envía a la gerencia para que sea aprobado.

- GERENCIA O&M

- *Aprobar plan de mantenimiento preventivo:*

  La gerencia revisa el plan propuesto y de no tener observaciones aprueba.

- *Envío del plan aprobado:*

  La gerencia envía a la jefatura y al área de desempeño el plan aprobado.

  - *DESEMPEÑO DE RED*

- *Incorpora el plan de mantenimiento al sistema:*

  Personal de desempeño registra en el sistema el plan de mantenimiento preventivo para su cumplimiento en las fechas propuestas.

  - O&M ISP JEFATURA

- *Registrar el plan y envía el cronograma autorizado:*

  La jefatura registra el plan en la carpeta FILE de ISP y envía al grupo de trabajo O&M ISP para la ejecución en las fechas propuestas.

  - O&M ISP GRUPO DE TRABAJO

- *Recepción del cronograma actualizado:*

  El grupo de trabajo de O&M recibe el plan de mantenimiento autorizado.

  Se ejecuta el cronograma en base a proceso “EJECUCION MANTENIMIENTO PREVENTIVO CRITICIDAD BAJA”

- Cierre de Ticket.

Ejecutar Cronograma Mantenimiento Preventivo
Criticidad Baja equipo Borde Quito

- O&M ISP JEFATURA

- *Solicitar ejecución de mantenimiento preventivo de la plataforma:*

  La jefatura solicita al grupo de trabajo O&M ISP ejecutar el plan de mantenimiento propuesto para el equipo Borde de Quito.

- O&M ISP GRUPO DE TRABAJO

- *Ejecutar órdenes de trabajo de mantenimiento preventivo:*

  El grupo de trabajo de O&M ejecuta la orden de trabajo de mantenimiento preventivo del equipo Borde de Quito, dentro de las actividades realiza la rutina de los indicadores de falla criticidad baja.

- *Toma de Decisión: Existe novedades?*

  El grupo de O&M no tiene novedades del equipo Borde de Quito.

- *Elaborar reporte de cumplimiento:*

  El grupo de O&M elabora el reporte de cumplimiento de la ejecución de mantenimiento preventivo del equipo Borde de Quito.

- O&M ISP JEFATURA

- *Revisar reporte, consolidar para mensual:*

  La jefatura revisa el reporte de cumplimiento de la ejecución de mantenimiento preventivo del equipo de Borde de Quito, consolida, elabora

el reporte mensual y envía a la gerencia.

- GERENCIA O&M

- *Recepción del informe mensual de cumplimiento de cronograma de mantenimiento preventivo:*

  La gerencia revisa y confirma que sí se cumplió con el plan de mantenimiento preventivo.

- Cierre de Ticket.

- NOC

- *Recepción del informe mensual de cumplimiento de cronograma de mantenimiento preventivo:*

  La gerencia revisa y confirma que sí se cumplió con el plan de mantenimiento preventivo.

- Cierre de Ticket.

- **Respaldos de configuración.**

Para esta función de desarrolló un proceso:

Respaldos de Configuración equipo Core Quito

- O&M ISP RESPONSABLE

- *Solicitar configuración comandos de obtención de respaldos:*

  La persona O&M responsable solicita al grupo de trabajo configurar el path en el equipo de Core Quito para que permita obtener los respaldos de configuración cada 24 horas o cada vez que se guarde la configuración y enviar esta data a un servidor FTP.

- O&M ISP GRUPO DE TRABAJO

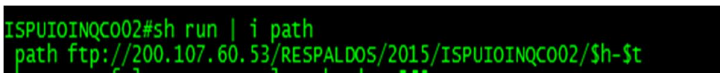
- *Configurar en los equipos de comunicaciones de ISP la obtención de respaldos y envío hacia un servidor FTP:*

  El grupo de trabajo de O&M configura en el equipo de Core Quito el path

- *Comprobar correcta ejecución:*

  El grupo de O&M comprueba que el comando se ejecutó correctamente, revisando que el path se encuentra creado.

  Como se muestra en la pantalla de abajo el path se encuentra creado.



- *Toma de Decisión: Respaldos Correctos?:*

  SI: El grupo de trabajo de O&M ISP revisa en el servidor FTP si se grabó la configuración realizada del equipo de Core Quito.

  Como se muestra en la gráfica de abajo el archivo se encuentra creado.

- Fin proceso.

  - O&M ISP RESPONSABLE

- *Revisar semanalmente la data del servidor FTP:*

  La persona O&M responsable revisa que el archivo esté guardado en el servidor FTP.

- *Toma de Decisión: Archivo actualizado y legible?:*

  SI: El grupo de trabajo de O&M ISP revisa el archivo que se encuentra en el servidor FTP comprueba que es legible, esta actualizado y que el ACL permite consultas SNMP, con esta actividad garantiza que los indicadores de falla definidos anteriormente están siendo monitoreados.

- Fin proceso.

➢ **Diagnóstico y Reparación.**

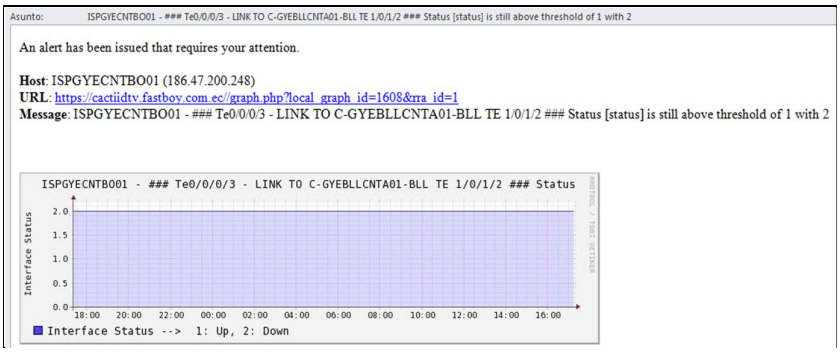
Para esta función de desarrolló dos procesos:

Mantenimiento Correctivo Criticidad Alta equipo Borde de Guayaquil

- CENTRO DE OPERACIONES NOC

- *Proceso "MONITOREAR INDICADORES DE FALLA CRITICIDAD ALTA":*

  El personal de NOC de acuerdo al proceso indicado recibe una alarma del indicador de Falla ESTADO FISICO DE LA INTERFAZ del equipo Borde de Guayaquil como se muestra en la gráfica, esto es debido al valor que se muestra en la Tabla3.1.2 del capítulo III (=2) para reportar una falla, como recibió valor 2 reportó.



Gráfica 4.1.14 Monitoreo indicador de Falla ï ESTADO FISICO DE LA INTERFAZ

- O&M ISP GRUPO DE TRABAJO

- *Intervención Nivel2:*

  El grupo de trabajo de O&M revisa logs en el equipo Borde de comunicaciones y detecta flapeos a nivel de protocolo, se contacta con personal de transmisión e informa que por un corte de fibra el momento de

empalmar manipuló la que corresponde a esta interfaz.

- *Toma de Decisión: Reparar Falla?:*

  SI: Personal de transmisión confirma al grupo de trabajo de O&M ISP que se encuentra superado el evento.

- El grupo de trabajo O&M ISP elabora el reporte de solución de la Falla indicando que es atribuible a un evento en el área de TX.

  El grupo de trabajo O&M ISP envía el reporte de la solución de la Falla a NOC indicando que es atribuible a un evento en el área de TX.

  - NOC

- *Recepta reporte de solución de Falla:*

  La persona NOC recepta reporte guarda en su bitácora.

- Cierra ticket

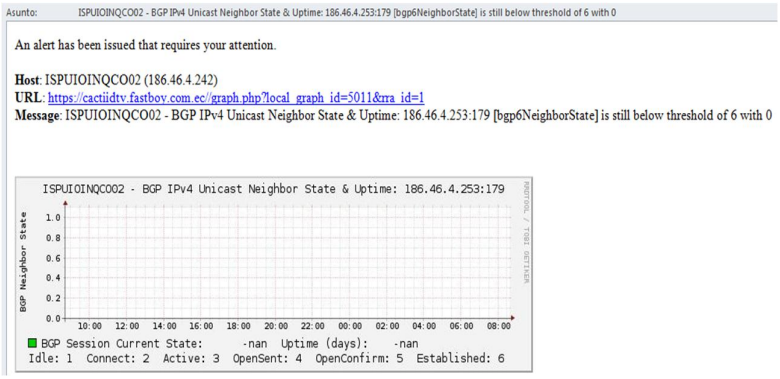
- Fin proceso.

Mantenimiento Correctivo Criticidad Media equipo Core de Quito

- CENTRO DE OPERACIONES NOC

- *Proceso "MONITOREAR INDICADORES DE FALLA CRITICIDAD MEDIA":*

El personal de NOC de acuerdo al proceso indicado recibe una alarma del indicador de Falla SESION BGP del equipo Core de Guayaquil como se muestra en la gráfica, esto es debido al valor que se muestra en la Tabla3.1.2 del capítulo III (≠ 6) para reportar una falla es diferente de 6.



Gráfica 4.1.14 Monitoreo indicador de Falla ï SESION BGP

- O&M ISP GRUPO DE TRABAJO

- *Intervención Nivel2:*

El grupo de trabajo de O&M revisa logs en el equipo Core de comunicaciones y no se registra eventos, se verifica la alarma del monitoreo y está devolviendo un valor nan, si la alarma hubiese enviado un valor entre 1 y 5 que son los pasos previos para el establecimiento de la sesión hubiese sido falla pero en este caso se recibió un valor nan por lo cual es únicamente

un problema en el monitoreo.

- *Reparar Falla2:*

  Personal de O&M ISP reconfigura en el monitoreo y se soluciona.

- El grupo de trabajo O&M ISP elabora el reporte de solución de la Falla indicando que es atribuible a un evento en el monitoreo y no causó afectación en la prestación del servicio.
- El grupo de trabajo O&M ISP envía el reporte de la solución de la Falla a NOC indicando que es atribuible a un evento en el monitoreo.
    - NOC
- *Recepta reporte de solución de Falla:*

  La persona NOC recepta reporte guarda en su bitácora.

- Cierra ticket / Fin proceso.

5. CAPITULO V – CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Se comprobó el Modelo de Gestión de Fallas aplicado sobre la herramienta CACTI mediante su opción de WEATHERMAP, la cual permite una visualización gráfica de la red de una manera rápida, refleja las alarmas, fácil consulta del estado de la red mediante la visión a nivel de colores de las gráficas correspondientes a cada nodo, segmento de equipos dentro del mismo y la notificación oportuna de las alarmas.

En este trabajo se identificaron 13 indicadores de gestión de fallas a los cuales se colocó umbrales, valores para reportar una falla, asociados a un nivel de criticidad para cada uno de los indicadores de falla, estos indicadores mejoran los tiempos de respuesta del área NOC.

Los procesos para el modelo de Gestión de Fallas desarrollados en este trabajo se alinean con la estructura organizacional de CNT EP, con la norma ISO 9000 (norma la calidad de redes), permitiendo definir claramente las actividades para cada área interna involucrada con el ISP y crear cultura de manejar procedimientos de gestión.

Los procesos desarrollados en este trabajo cumplen con las siguientes funciones de un modelo de Gestión de Fallas: supervisión del estado de la red, detección de

problemas, respaldo de configuración, diagnóstico y reparación.

Como resultados obtenidos en este trabajo se desarrollaron 3 procesos para la función supervisión del estado de la red, 2 procesos para la función detección de problemas, 1 proceso para la función respaldos de configuración y dos procesos para la función diagnóstico y reparación.

Los procesos desarrollados para cada función de la gestión de falla se muestran mediante diagramas de flujo lo cual permite de una manera gráfica identificar los actores, las actividades que corresponde a cada actor y sobre todo genera de manera formal responsabilidades para las áreas involucradas. Para su desarrollo se utilizó la misma herramienta con la cual CNT EP registra oficialmente los procesos (VISIO MICROSOFT).

Se realizó una prueba lógica de verificación de los procesos definidos para la Gestión de Fallas a un grupo de fallas ocurridas sobre el equipamiento de comunicaciones (routers) que conforman la plataforma de ISP comprobando que las actividades definidas en los diagramas de flujo de cada proceso son correctas.

5.2 RECOMENDACIONES

Implementar los procedimientos de Gestión de Falla definidos en este trabajo en la Jefatura de O&M de Core y Plataformas IDTV con la finalidad de optimizar recursos, mejorar tiempos de respuesta e incrementar disponibilidad.

Implementar los procedimientos de Gestión de Falla definidos en este trabajo en las demás áreas técnicas internas de la empresa como la de acceso MPLS y Backbone MPLS de Internet que son parte de la prestación del servicio de Internet.

Adquirir y utilizar otras herramientas de gestión de monitoreo que permitan correlacionar las fallas entre los equipos que conforman la red que permite la prestación del servicio, mejorando aún más los tiempos de atención de incidentes, mejorando la disponibilidad de la red ya que si bien CACTI es una ayuda no es una herramienta completa como un OSS (Operation Support Service).

6. BIBLIOGRAFIA

[1] Designing Cisco Network Service Architectures Vol 3, v2.1 2010, Lesson 2 (CISCO, 2010)

[2] www.cisco.com (CISCO, 2015)

[3] GESTION DE REDES .Pr (EGAS, 2007)

[4] Network Management: Principles and Practices (2nd Edition), Mani Subramanian, 2012(Subramanian, 2012)

[5] www.snmp.com (SNMP, 2015)

[6] EVOLUCIÓN DEL PROTOCOLO DE GESTIÓN DE INTERNET. Pr (MOLERO, 2010)

[7] INTERNETWORKING WITH TCP/IP, Douglas E. Comer, 2014 (COMER, 2014)

[8] Página WEB de CACTI (http://www.cacti.net) (CACTI, 2015)

[9] Norma ISO9001:2008 (http://www.iso.org)(ISO, 2008)

[10] http://corporativo.cnt.gob.ec/wp-content/uploads/2014/11/a_Estructura_Organizacional_CNT_EP-2014.pdf (www.cnt.gob.ec, 2014)

[11] Norma ISO9001:2008 (http://www.iso.org) (ISO, 2008)